Springer Series in Supply Chain Management

George A. Zsidisin
Michael Henke *Editors*

Revisiting Supply Chain Risk

Springer

Springer Series in Supply Chain Management

Volume 7

More information about this series at http://www.springer.com/series/13081

George A. Zsidisin · Michael Henke
Editors

Revisiting Supply Chain Risk

Springer

Editors
George A. Zsidisin
Virginia Commonwealth University
Richmond, VA, USA

Michael Henke
TU Dortmund University, Fraunhofer
Institute for Material Flow and Logistics
IML
Dortmund, Germany

ISSN 2365-6395 ISSN 2365-6409 (electronic)
Springer Series in Supply Chain Management
ISBN 978-3-030-03812-0 ISBN 978-3-030-03813-7 (eBook)
https://doi.org/10.1007/978-3-030-03813-7

Library of Congress Control Number: 2018961700

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Dedication

Revisiting Supply Chain Risk is dedicated to the memory and work of Prof. Bob Ritchie. We were made aware of Bob's passing at the end of the Summer 2016 and were very sad to hear this news, but also honored to have known and worked with him as a colleague and friend. It was our mutual curiosity of supply chain risk that brought us together, and with a several others (Andreas Norrman, Ulf Paulsson) formed the foundation of the International Supply Chain Risk Management (ISCRiM) network in October 2001. During our annual meeting in 2017, which was hosted by Markus Gersberger in Styer, Austria, we decided to co-edit a book dedicated to Bob, commemorating 10 years since the publication of "Supply Chain Risk: A Handbook of Assessment, Management and Performance" by George Zsidisin and Bob Ritchie. In Bob's memory, we would like to share the historic origins of ISCRiM and Bob's leadership, work, and dedication to the network, which is still today an active organization focusing on advancing our knowledge of supply chain risk.

During the summers between my third and final year as a Ph.D. student at Arizona State University, I (George Zsidisin) attended a jointly held conference combining the International Purchasing and Supply Education and Research Association (IPSERA) and the North American Research and Teaching Symposium (NARTS; previously sponsored by the Institute for Supply Management) in London, Ontario, Canada, in 2000. During the conference, I presented a paper outlining some of my work and initial insights from my dissertation on supply risk perceptions and management. Likewise, another paper was presented at the same session by John Morris, a colleague of Bob Ritchie's, providing some initial thoughts on the underdeveloped (at that time) topic of supply chain risk. After sharing some initial discussions about supply chain risk, we left the conference with promises to stay in touch on this subject area.

Near the same time frame, I received an email from Robert Lindroth, a Ph.D. student at Lund University (working with Andreas Norrman and others), who was studying supply chain risk for a semester at Stanford University. He referenced one of my initial publications that just came out on the subject and shared some insights on the research programs we were working on associated with supply chain risk.

From these initial contacts, Bob Ritchie, Andreas Norrman, and I, in conjunction with a few others (i.e., Ulf Paulsson), decided to meet in person to discuss the emerging topic of supply chain risk in Crewe, UK, on October 11, 2001. Bob was kind enough to host the first meeting, especially since I was a very junior professor just taking my first academic position. Of course, one month prior to our meeting, the world experienced the devastation of 9–11, which still has significant ramifications in the way we manage supply chains and live our everyday lives. The initial meeting was almost canceled, but we ultimately decided to keep our plans.

In recent seminars, we have been accustomed to the general structure of having an evening prior reception, and then having presentations, discussions, and meetings lasting one and a half days. For our first meeting, we met for three days. We did not know what to expect, since we were all still relatively novice scholars in this area, and there were only a few prior studies done on risk from a supply chain context (going beyond inventory models). It is from the initial meeting that we decided: (1) the name International Supply Chain Risk Management (ISCRiM) network, (2) to host annual meetings/seminars to update each other as to the work we are doing on supply chain risk, (3) the structure of the network would be informal, though with a few ground rules, such as civil/constructive dialogue in presenting our work, (4) to slowly grow the network, (5) contribute our initial work to our first book, which was edited by Clare Brindley in 2004, and (6) meet the following year in Lund, Sweden.

From this initial meeting a seed was planted, with Bob cultivating this network with several others throughout the years. In reflecting the history, we have met annually at various locations, starting from the most recent: Lappeenranta, Finland (2017); Steyr, Austria (2016); Richmond, Virginia, USA (2015); Dortmund, Germany (2014); Verona, Italy (2013); Porto, Portugal (2012); Denton, Texas, USA (2011); Loughborough, UK (2010); Cullowhee, North Carolina, USA (2009); Trondheim, Norway (2008); Lappeenranta, Finland (2007); Oestrich-Winkel, Germany (2006); Cranfield, UK (2005); East Lansing, Michigan, USA (2004); Crewe, UK (2003); Lund, Sweden (2002); and Crewe, UK (2001).

Bob and I would occasionally correspond on details and meeting locations of ISCRiM, and well as projects. I was honored to co-edit my first book with Bob, in conjunction with the work of many members of the ISCRiM community contributing their scholarship. Bob served the critical role in soliciting and attaining Springer to publish our book. I still remember the detailed coordination with Bob, the various authors, and the publishers to ensure the successful completion and distribution of the book, simply titled "Supply Chain Risk: A Handbook of Assessment, Management, and Performance." I still have copies in both my home and work offices. Just simply looking at the long list of contributors reminds me of all the lives Bob has touched in his life, and especially, from my personal knowledge, the ISCRiM community. The work and curiosity on supply chain risk was the initial bond both Bob and I shared. However, one other passion Bob and I shared was a love of music.

In communications with his wife, Celia, we learned that Bob, during his youth, formed a band called "The Ranters." What a name for a band, and especially, given the hazards of our profession, we may tend to "rant" a little! We first learned of Bob's interest in music interest during our seminar in North Carolina. We still remember Bob and several others passing a guitar around and singing songs during our seminar in Cullowhee, NC, as well as our share of spirits—a very fond and memorable moment.

When we learned of Bob's passing, we sent out a request for contributions to the ISCRiM newsletter reflecting on the work and life of Bob Ritchie. Below are two of the notes from ISCRiM members:

> I was deeply saddened to hear that we'd lost Bob. Many of us who knew him will be reflecting on the contributions he made to ISCRiM, both in terms of his research and his support for the network. Most of all though, I remember him for the person he was. In an age where the word 'nice' is often used as a simile for 'underwhelming,' and unkind and boorish behaviour seems to be increasingly acceptable in the public domain, I shall remember Bob for being the opposite. He was a genuinely, relentlessly, nice man. My fondest memories of him are from the ISCRiM seminar at Lake Junaluska, NC. Signs of his illness were starting to affect the volume control of his voice (prompting periodic hand signals from me to remind him to up the volume). He took this in his stride. Likewise, when most of the group had gone home, Mike Smith, his wife Brigid and their youngest son took us sightseeing—involving a walk to a hill top beauty spot, as well as dinner at their home. The dinner and views were both lovely, but what I shall remember most is watching how Bob's gentle, encouraging good humor effortlessly drew the whole family to him. His passing is very much our loss.
>
> —Helen Peck

> I met Bob Ritchie in person when I participated for the first time in the ISCRiM-Seminar in 2004 in Cranfield. In the following years, we have built up a very cooperative and friendly relationship. Bob on a personal level encouraged me to sharpen my research focus on supply risk and supply chain risk management. Owing to his always polite and helpful nature, he was not only my role model but also of many colleagues. He made a decisive contribution to establish and expand research in the field of supply (chain) risk management—within the ISCRiM community and far beyond. I gladly think back to the hours spent together and I will miss Bob.
>
> —Michael Henke

We also asked Celia Richie, Bob Ritchie's wife, if she would like to write a few words in memory of her husband. It can be found below. In addition, she was kind enough to share a photo of Bob.

> My son, Jason, and I are very proud of all Bob's academic achievements. He was always willing to listen and help others, inside and outside of the academic world. He had time and patience for everyone and would be humbled by the numerous contributions from the scholars for the publication of this book. A fitting tribute to his working life in education.
>
> However, despite all of his achievements, he was my Bob, my husband, a father and grandfather, loved by us all and greatly missed.
>
> —Celia Ritchie

ISCRiM has taken a life of its own since its initial first meeting in 2001. Professor Bob Ritchie had the vision of inviting some of the earliest scholars to share their perspectives on this emerging topic, which has significantly grown in recognition and knowledge during the past two decades. We will always be appreciative of Bob's work, insight, laid-back style, sharing, and friendship. We will continue to build from his foundational work and recognize his influence in our scholarship and lives. This book is a testament to his work and is only possible from the foundations he laid. Thank you, Bob—you are missed, but always alive in our memories and in our work.

Contents

About the Editors

George A. Zsidisin, Ph.D. (Arizona State University), CPSM, C.P.M., is a Professor of Supply Chain Management at Virginia Commonwealth University. He has conducted extensive research on how firms assess and manage supply disruptions and commodity price volatility in their supply chains. He has published over 80 research and practitioner articles that have been extensively cited, many of which focus on the topic of supply chain risk and continuity management. His research on supply chain risk has been funded by the AT&T Foundation and IBM and has received numerous awards, such as from the Institute for Supply Management, Deutsche Post, Council of Supply Chain Management Professionals, and the Decision Sciences Institute. He has edited two other books: *Supply Chain Risk: A Handbook of Assessment, Management, and Performance* (with Bob Ritchie, 2009), Springer International Publishing; and *Handbook for Supply Chain Risk Management: Case Studies, Effective Practices and Emerging Trends* (with Omera Khan, 2012), J. Ross Publishing. In addition, he has published *Managing Price Volatility: a Supply Chain Perspective* (with Janet Hartley, 2012; second edition 2017), Business Expert Press Publishing, with translated versions in German (with Lutz Kaufmann) and Italian (with Barbara Gaudenzi). He has served as a Co-director for the Supply Chain Leadership Program for the Purchasing Management Association of Canada, is one of the initial founding members of the International Supply Chain Risk Management (ISCRiM) network, and has taught and led discussions on supply chain management and risk in various executive education programs and numerous companies in the USA and Europe. He is a co-Editor Emeritus of the Journal of Purchasing & Supply Management, is the Director of the Master of Supply Chain Management program at Virginia Commonwealth University, and sits on the Editorial Review Board for several academic supply chain journals.

Prof. Dr. Michael Henke is the Director of Fraunhofer Institute for Material Flow and Logistics IML in Dortmund and is the Chair in Enterprise Logistics (LFO) at the Faculty of Mechanical Engineering at TU Dortmund University, Germany. Furthermore, he is Adjunct Professor for Supply Chain Management at the School of Business and Management of Lappeenranta University of Technology in Finland. His research focuses inter alia on Management of Industrie 4.0 and Platform Economy, Blockchain and Smart Contracts, Financial Supply Chain Management, Supply Chain Risk Management, Procurement, Logistics and Supply Chain Management. Doing this, he is combining his practical experience from entrepreneurial practice and his extensive knowledge from research. He studied Brewing and Beverage Technology (Dipl.-Ing.) and gained his doctorate and habilitation in Business and Economics at Technical University of Munich, Germany. During and after his habilitation, he worked for the Supply Management Group SMG in St. Gallen, Switzerland. From 2007 until 2013, he was active in teaching and research as a Professor at European Business School (EBS).

Chapter 1
Research in Supply Chain Risk: Historical Roots and Future Perspectives

George A. Zsidisin and Michael Henke

1 A Rich and Developing History

Risk has always existed in business and supply chains—well before the terms supply chain and supply chain management became part of our lexicon. There is no shortage of reported incidents from centuries and even millennia ago about supply disruptions due to shipwrecks from storms or piracy/theft from transporting spices, food, precious metals, materials, and a myriad of other products. Simply stated, throughout history we have been challenged with managing risk in our supply chains.

The interest in and study of supply chain risk can be argued to have started shortly after the emergence of supply chain management as a recognized academic discipline in business. Prior research associated with supply chain risk, usually in the form of disruptions, focused on providing certain service levels through inventory management (minimizing stockouts) or determining when to use one or multiple suppliers. However, our understanding of supply chain risk and its management (beyond creating inventory buffers and multiple supply sources) as an academic area of inquiry has only emerged with changing business practices and world events starting around the turn of the twenty-first century.

During the last 20 years, we have significantly expanded our knowledge and awareness of supply chain risk. A thorough review of this rich literature is well beyond the scope of this introduction chapter. However, the contributions throughout this book build on and cite most of the seminar published studies in this discipline.

G. A. Zsidisin (✉)
Department of Supply Chain Management and Analytics, Virginia Commonwealth University, Richmond, USA
e-mail: gazsidisin@vcu.edu

M. Henke
TU Dortmund University, Fraunhofer Institute for Material Flow and Logistics IML, Dortmund, Germany
e-mail: michael.henke@iml.fraunhofer.de

G. A. Zsidisin and M. Henke (eds.), *Revisiting Supply Chain Risk*, Springer Series in Supply Chain Management 7, https://doi.org/10.1007/978-3-030-03813-7_1

Today, we are observing an unprecedented shift in our ability for detecting, preventing, and mitigating the detrimental effects of supply disruptions and other forms of risk (financial, reputation). Industry 4.0, with its technological emphasis on digitization, connectedness, and data analysis capabilities, arguably provides the next platform for us in our ability to identify, analyse, estimate, and proactively manage supply chain risk from the n-tier supplier to the final consumer.

2 Shifting Toward Digitalization and Data Analytics

Since the last significant financial and economic crisis in 2008, many enterprises established crisis management approaches best described as reactive, instead of focusing on proactive risk management approaches for rectifying issues such as supplier insolvencies (Henke et al. 2010). However, with the recent technological leaps of digitalization and (big) data analytics, firms have significantly greater capability for creating comprehensive and proactive supply chain risk management (SCRM) processes in business practice.

Since the fourth industrial revolution is continuing to push information and communication technology even further, its enabling technologies provide the ability for realizing real-time SCRM. Digital supply chains provide extensive information availability and enable superior collaboration and communication because of the technological integration of processes and systems, creating an interconnectedness at every integral part of a supply chain (Raab and Griffin-Cryan 2011). Digitalization facilitates a dynamic manufacturing system, making networking across company borders possible and generating transparency. The digital supply chain makes it possible to identify potential sources of risk and implement mitigation plans efficiently in complex networks, since material, information, and financial flows are “visible” in real time and detail (Butner 2010; Yu and Goh 2014).

Real-time information availability in combination with corresponding data-processing tools allows a faster reaction to changing conditions along the supply chain (Güller et al. 2015). With this technological evolution, it is possible to rather accurately anticipate near future changes. In this context, big data analytics and real-time decision-making allows companies to react to the fast-changing business environment, since it provides insight from data by applying statistics, mathematics, econometrics, simulations, optimizations, or other techniques (Wang et al. 2016). With the help of big data analytics, information is converted into business intelligence, which leads to a better understanding of events from the past but also to predict future events (Sanders 2014). In that case, predictive analytics provide estimations about the future state using business forecasting and simulation to answer questions of “what will happen?” and “why will it happen?” (Delen and Demirkan 2013). Prescriptive analytics is used to recommend a course of mitigation actions for given the predicted future by using simulation and optimization and addresses questions such as “what shall we do?” and “why shall we do it?” (Evans 2012). Predictive analytics captures relationships among many factors to assess risk and utilizes patterns found between historical and transactional data to identify future potential vulnerabilities (Seuring and Müller 2008). On the other hand, with optimization, simulation, and scenario analysis, prescriptive analytics proposes mitigation actions to avoid risk in situations that will be faced in future (Rozados et al. 2014). As a result, big data analytics have great opportunities for analysis of large-scale data to help companies in risk management and decision-making.

A technology which has been promoted in recent months and which may help in identifying and managing supply chain risk is blockchain technology. With the potential to serve as an appropriate transaction layer for information, blockchain is able to build a digital backbone with IoT and increase visibility into the structure of extended supply chains (Schrauf and Berttram 2017; Biswas and Sen 2016; Babich and Hilary 2018). Blockchain technology can play a central role in SCRM processes (Babich and Hilary 2018). In blockchain-based supply chains, the origin of products can be verifiable and every object in the supply chain provides an unchangeable recording of its activities, also allowing backtracking of actions (Satyavolu and Sangamnerkar 2016). With this increased supply chain visibility, companies can discover potential bottlenecks, estimate probabilities of adverse events, and forecast their consequences at an early stage (Babich and Hilary 2018). Unlike conventional enterprise solutions, where the relevant data is stored in a centralized and isolated manner, Blockchain is a distributed ledger technology, which has the ability to securely digitize many current operations and to share all transaction information between network parties (Yoo 2017). This elimination of information asymmetries allows a shift toward data-driven SCRM and demands further investigation on the role of new information structure for SCRM processes (Babich and Hilary 2018).

Revisiting Supply Chain Risk, as a collection of current research, practice, and philosophy, in many ways serves as a bridge between our current understanding of supply chain risk in practice and theory, and the monumental shifts we are seeing with the emergence of the fourth industrial revolution. Many of the following chapters in the book either directly provide tools or approaches, or indirectly acknowledge the importance and criticality of big data analytics in SCRM processes.

3 Structure of the Book

The study of supply chain risk and its management has significantly developed and branched out to many areas. The ISCRiM network published its first edited book by Brindley (2004), and subsequently Zsidisin and Ritchie (2009) and Khan and Zsidisin (2012). Further, other edited books have further advanced our understanding of supply chain risk, including those from Wu and Blackhurst (2009), and Sodhi and Tang (2012). In addition, almost all supply chain management academic journals and have published numerous research articles on supply chain risk and its various components and related phenomenon. These topics include, but are by no means limited to, supply chain resilience, supply chain vulnerability, supply continuity planning and disruption management, digitization/Industry 4.0 (as previously discussed), supplier risk management, trust, relationships, culture, quality, commodity price volatility, foreign exchange risk, supply chain network design, cyber security, information management, and risk assessment, among others.

Many of the chapters in this collection likewise can be categorized into one or many of these sub-disciplines or related subjects with supply chain risk. As co-editors, we made some difficult decisions in determining the most appropriate section to place each chapter. We believe the current contributions highlight both established themes in the supply chain risk literature (Assessing Supply Chain Risk; Creating Resiliency by Managing Supply Chain Risk), as well as provide new insights into the developing areas of inquiry and contexts in supply chain risk (Incorporating Relational and Behavior Perspectives; Managing Risk in Sustainable and Innovative Supply Chains). Further, we noticed several chapters proposing new typologies and taxonomies of how we understand supply chain risk, building on the foundation of published research in this field. The concluding section provides some grounded cases and thought pieces to provide insight into actual company practices and current academic thought in supply chain risk.

The book is structured into six main sections reflecting themes emerging from the content of the contributed chapters. These themes are:

1. Assessing Supply Chain Risk—The First Step in Managing Supply Chain Risk
2. Creating Resiliency by Managing Supply Chain Risk
3. Incorporating Relational and Behavioral Perspectives
4. Managing Risk in Sustainable and Innovative Supply Chains
5. Emerging Typologies and Taxonomies
6. Grounding Our Understanding of Supply Chain Risk: Cases and Observations

3.1 Assessing Supply Chain Risk—The First Step in Managing Supply Chain Risk

Numerous models and processes have been published describing the importance of assessing supply chain risk exposure in order to provide insight as to how to best manage risk (Zsidisin et al. 2000, 2004; Norrman and Jansson 2004; Jüttner et al. 2003; Tummala and Schoenherr 2011). The continued growth of computing power and data storage capabilities, the development of advanced data analytic techniques, and the growth of third party supply chain risk management consultants and software have provided scholars and practitioners an unprecedented opportunity for better assessing risk in the supply chain. The following chapters reflect these increased capabilities for assessing supply chain risk.

Chapter 2—Assessing the Vulnerability of Supply Chains: Advances from Engineering Systems—authored by Sigurd S. Pettersen and Bjørn Egil Asbjørnslett, provides emerging trends and advances from engineering design for assessing supply chain vulnerabilities. Advances discussed in the chapter include epoch-era analysis for structuring of event taxonomies and scenarios, failure mode thinking for low-frequency, high-impact (LFHI) events, and design structure matrices and axiomatic design principles for function–form mapping in the supply chain.

In Chap. 3—Using Scenario Planning to Supplement Supply Chain Risk Assessments—Cliff Thomas and Thomas Chermack propose the use of scenario planning as a supplement to traditional supply chain risk assessment paradigms and practices. The chapter provides evidence and arguments for scenario planning as a viable approach for raising and enhancing the level of supply chain risk awareness among decision-makers.

Chapter 4—Decision Support Systems and Artificial Intelligence in Supply Chain Risk Management—authored by George Baryannis, Samir Dani, Sahar Validi, and Grigoris Antoniou, argues the importance of decision support systems for analyzing and subsequently managing supply chain risk. The chapter first provides an overview of the different operations research techniques and methodologies for decision-making associated with managing risk, focusing on multiple-criteria decision analysis methods and mathematical programming. Artificial intelligence (AI) techniques, such as Petri nets, multi-agent systems, automated reasoning and machine learning, are also applied for making decisions associated with supply chain risk.

The final chapter in this section, in Chap. 5—Resilience Assessment in Complex Supply Networks—authors Mustafa Güller and Michael Henke define and formalize a method for a holistic resilience assessment in complex supply networks. Their assessment methodology incorporates supply chain design, supplier related factors, relational competencies, and physical and capital resources for calculating a quantitative rating of supply chain resilience.

3.2 Creating Resiliency by Managing Supply Chain Risk

Supply chain resilience has been defined by as Svensson (2002) as "unexpected deviations from the norm and their negative consequences." Resiliency from disruptions, significant price valuations, and other forms of risk have been at the forefront as a critical outcome from reducing vulnerability and managing risk (Pettit et al. 2010).

The section begins with Chap. 6—What Value for Whom in Risk Management?—A Multi-value Perspective on Risk Management in an Engineering Project Supply Chain—authored by Pelle Willumsen, Josef Oehmen, Monica Rossi, and Torgeir Welo. This chapter presents a conceptual model for developing supply chain risk management activities that are based on the value perspectives of key stakeholder groups in a customer–supplier relationship. The authors discovered that taking into account stakeholder value propositions when designing supply chain risk management processes is beneficial for identifying conflicting value profiles and leveraging shared ones, and hence, enabling the customization of these processes to ensure value from multiple perspectives.

Chapter 7—Risk Management of Critical Logistical Infrastructures: Securing the Basis for Effective and Efficient Supply Chains—authored by Michael Huth and Sascha Düerkop, develops a risk evaluation approach for critical logistics infrastructures. The evaluation considers how the limitation or breakdown of any element of a logistics network influences all supply chains using the network. By calculating risk-induced cost for the supply chains, implications of risk can be quantified and used as a basis for decision-making.

Chapter 8—Procedure Model for Supply Chain Digitalization Scenarios for a Data-Driven Supply Chain Risk Management—written by Florian Schlüter, presents a process model supporting management in developing and assessing supply chain process-oriented digitalization scenarios with a focus on risk prevention and reduction. Decision-makers can decide between different maturity stages for managing supply chain risk and develop digitalization scenarios in workshops supported by domain mapping matrices to structure the process

Chapter 9—Preparing for the Worst, authored by Yossi Sheffi—provides an updated perspective from his prior work in how companies are now managing supply chain risk. The chapter illustrates four common categories of investment, each of which can be looked upon as a real option, companies make in preparation for disruptions in supply or surges in demand. The categories are investments in redundancy (e.g., inventory), flexibility (i.e., of facilities and processes), emergency operation centers (EOC), and business continuity planning (BCP).

The second section concludes with Chap. 10—The Future of Resilient Supply Chains—contributed by Mattia Donadoni, Sinéad Roden, Kirstin Scholten, Mark Stevenson, Federico Caniato, Dirk Pieter van Donk, and Andreas Wieland. Their chapter investigates what managers understand as disruptions and resilience and how they measure these constructs. Practitioners focus on operational risks or challenges that occur on a daily basis (low impact, high probability) rather than focus on potentially more impactful disruptions with wider spread consequences (high impact, low probability). Further, they may be reluctant to dedicate resources for pursuing strategies enhancing resilience if they are not able to prove the return or benefits that they will obtain in the long term.

3.3 Incorporating Relational and Behavioral Perspectives

It can be argued that some of the initial research in supply chain risk focused on the effects of risk at the firm level, and oriented toward organizational processes and systems to prevent or mitigate the effects of risk on firm performance. However, there is also the human element which becomes an important factor in going beyond processes themselves and beginning to understand the relational and behavioral elements influencing supply chain risk exposure, as well as how it is viewed and managed. This section looks at those relational and behavioral perspectives from varying units of analysis, including consortiums, teams and individual leaders and decision-makers.

The section begins with Chap. 11—Can Buyer Consortiums Improve Supplier Compliance?—authored by Felipe Caro, Prashant Chatapalli, Kumar Rajaram, and Christopher S. Tang. This chapter discusses the use of joint audit mechanisms done by buyer consortiums when suppliers fail to comply with environmental or safety regulations. Findings from their research suggest a joint audit mechanism is beneficial by increasing supplier compliance levels, and can increase profits when the audit cost is below a certain threshold.

Chapter 12—Leadership in Risky Supply Chains—written by Christopher R. Paparone and George L. Topic Jr., provides insight into how adaptive leaders exercise "creative deviance" and seeks to influence others in the chain to diverge from their habitualized frames of reference through divergence and value patterning when encountering risk in the supply chain. However, while adaptive leadership becomes a mitigation strategy for confusingly novel situations, there are also social risks for supply chain innovators.

In Chap. 13—Malicious Supply Chain Risk: A Literature Review and Future Directions—Scott DuHadway and Steven Carnovale examine intentional disruptions arising from deliberate actions that can negatively affect supply chain operations and performance. In order to manage this risk, the authors provide a framework encapsulating a three-pronged approach centered on (1) avoiding and detecting, (2) mitigating the impact of, and (3) recovering from this unique type of supply chain risk.

The section concludes with Chap. 14—A Behavioral View of Supply Chain Risk Management—written Mehrnoush Sarafan, Brian Squire and Emma Brandon-Jones. This chapter questions the implicit assumptions of rational decision-making, consistent preferences, and optimal choice in prior supply chain risk research, and argues from other lines of research that environmental uncertainty and managerial illusions create deviations from rational decision-making. Further, some of these studies have found managers may have individual goals not related to risk and cost minimization but instead reflect their risk preferences, status-seeking, or the history of their relationships with exchange partners. This chapter draws from advances in behavioral research to highlight the importance of incorporating such factors into supply chain risk management models.

3.4 Managing Risk in Sustainable and Innovative Supply Chains

There have been several topics in supply chain management practice and research which have been receiving increasing attention during the last two decades. First, it can be argued that the study of sustainability in supply chain management has received as much, or maybe even more attention in research agendas during the last twenty years. Although a few earlier studies have made mention of sustainability as a source of risk (Zsidisin 2003), it has only been during the last few years we have seen a convergence of sustainability and supply chain risk literatures. The first two chapters of this section focus on sustainability with regard to supply chain risk.

Innovation is likewise a critical business process and has received extensive attention in the literature in the Marketing and Operations Management literatures. However, there appears to be limited knowledge of innovation from a supply chain perspective, especially with regard to risk. Innovation can be argued as serving as an enabler for creating more efficient and effective supply chains, to include reducing the likelihood of disruptions, but also potentially as a cause of supply chain risk. The latter two of the chapters focus on the linkage between innovation and managing supply chain risk.

In Chap. 15—Resilience and Sustainability in Supply Chains—Holmes E. Miller and Kurt J. Engemann present an overview of issues regarding supply chain resilience and sustainability, and how the two interact. The resilience-sustainability relationship is presented with possible cost/benefit categories, analogous to the total cost of quality categories: operational, compliance, direct, and indirect. These categories can serve as a basis for informing decision-makers when seeking to make decisions regarding resilience–sustainability strategies.

Chapter 16—Sustainability Risk Management in Supply Chain—authored by Jukka Hallikas, Katrina Lintukangas, and Daniela Grudinschi, investigates practices for implementing and assuring responsibility in the purchasing and supply chain and the role of risk management in assuring that responsibility. These practices, based on case study observations, identify and prioritize the most important sustainability issues and implement the actions required to manage risk during the procurement process phases of strategic planning, assessing and selecting suppliers, contracting, monitoring and measuring, developing and assessing supply, and cooperating and networking

Focusing on innovation and risk, in Chap. 17—The Relationship Between Firm Resilience to Supply Chain Disruptions and Firm Innovation—Mahour M. Parast, Sima Sabahi and Masoud Kamalahmadi discuss the relationship between supply chain disruption risk management and innovation management and examine whether a firm's investment in innovation can improve the firm's resilience to supply chain disruption. Findings from a literature review suggest leadership, information sharing, and collaboration as practices that improve both firm innovation and firm resilience from supply chain disruptions.

Chapter 18—Supply Chain Virtualization: Facilitating Agent Trust Utilizing Blockchain Technology—authored by Kane Smith and Gurpreet Dhillon, discuss the use of blockchain technology as a mechanism for facilitating trust between various supply chain agents. This innovation gives supply chain entities within the blockchain a copy of the information record, which cannot be altered without their consent, as well as serves as a secure method of encryption providing protection against tampering from malicious sources and security of the information contained on the chain.

3.5 Emerging Typologies and Taxonomies

Typologies and taxonomies of supply chain risk and supply chain risk management processes started to emerge approximately fifteen to twenty years ago (Mitchell 1995; Svensson 2000; Zsidisin et al. 2000; Jüttner et al. 2003; Zsidisin 2003; Zsidisin and Ellram 2003; Tang et al. 2006; Henke 2009). The sheer growth in the number of publications since then examining different facets of supply chain risk has allowed for creating approaches for categorizing the studies themselves, similar to a meta-analysis of published studies. These "studies of studies" are arguably a step toward consolidating our understanding of supply chain risk and its many facets. The three chapters in this section provide insight into the most current thought of classifying supply chain risk.

This section begins with Chap. 19—Differentiating Between Supply and Supplier Risk for Better Supply Chain Risk Management by Sudipa Sarker. In this chapter, the author uses both prior studies as well as case studies of firms to discern the differences in units of analysis of where risk stems from in the upstream supply chain.

Chapter 20—Categorizing Supply Chain Risks: Review, Integrated Typology and Future Research—written by Mihalis Louis and Mark Pagell, argues that firms looking to guarantee their long-term survival need to successfully identify risk in their supply chain. This chapter examines the types of risk in the supply chain by reviewing the various typologies proposed in the SCRM literature since 2000 using the Systematic Network Analysis method. The results of the analysis propose a new typology of supply chain risk that is both inclusive and parsimonious.

The final chapter of this section, Chap. 21—The Impact of Supply Chain Disruptions on Organizational Performance: A Literature Review—by Mahour M. Parast and Mansoor Shekarian, identifies different conceptualizations and theorizations of supply chain disruptions in order to understand how they affect organizational performance. The authors argue organizational capabilities of flexibility, agility, collaboration, and redundancy serve as resilience enhancers that can improve an organizational response to supply chain disruptions.

3.6 Grounding Our Understanding of Supply Chain Risk: Cases and Observations

The final section of the book starts with providing three chapters of illustrative cases in assessing and managing supply chain risk. The last two chapters are best described as thought pieces by providing new insights and applications for our understanding of supply chain risk.

First, in Chap. 22—The Management of Disruption Supply Risk at Vestas Wind Systems—Chris Ellegaard and Anne Høj Schibsbye propose a flexible supply risk management framework for helping managers mitigate disruption risk. The case study, gleaned from analyzing the purchases of gearboxes, towers, and electronics, shows how different sets of strategies are required for the successful mitigation of risk. Effective disruption mitigation may require different strategies depending on the type of supply and the varied drivers causing the disruption.

In Chap. 23—Foreign Exchange Risk Mitigation Strategies in Global Sourcing: The Case of Vortice SPA—the authors Barbara Gaudenzi, Roberta Pellegrino, George A. Zsidisin and Claudio Bruggi examine supply chain approaches at Vortice SPA for mitigating FX risk. This case study of a small- and medium-sized enterprise describes how the firm utilizes a mix of financing and contracting strategies to reduce the detrimental financial effects associated with currency rate fluctuations.

In the third chapter of this section, Chap. 24—The Paradox of Risk Management: A Supply Management Practice Perspective by Sudipa Sarker—describes how different risks are managed using a multitude of methods during diverse activities within the supply management process by different personnel positioned at various hierarchical levels of the organization.

In Chap. 25—Risk in Complex Supply Chains, Networks and Systems—Christine Mary Harland examines issues and challenges facing complex interorganisational networks and systems that straddle public and private sectors, and explore risks and mitigation specific to these types of network. These examples are used to form an initial conceptual framework for future empirical research.

The concluding Chap. 26—Surfing the Tides of Political Tumult: Supply Chain Risk Management in an Age of Governmental Turbulence—by Michael E. Smith provides an overview of political strategy for SCRM and how competencies can be developed to help organizations deal with the uncertainties inherent in political turbulence. Three sources of risk: (1) acts of government commission, (2) acts of government omission, and (3) political acts of players outside of government, create a challenging environment in which organizations must attempt to identify, understand, and seek to develop responses adequate for its management.

4 Conclusions

As long as we will have businesses, organizations, and supply chains, we will likewise have risk associated with the various product, information, and financial flows within and among these entities. The study of risk in the supply chain has taken on greater importance as firms continually improve their processes and capabilities in meeting ever-increasing demands and requirements from customers. Our goal in *Revisiting Supply Chain Risk* is to provide you, the reader, current research and philosophical thought in supply chain risk, and where we are heading as a discipline in the future. A significant part of this future may well lie in the capabilities the fourth industrial revolution may serve in creating more robust SCRM processes. We hope the following chapters achieve this goal.

References

Babich, V. R., & Hilary, G. (2018). *Distributed ledgers and operations: What operations management researchers should know about blockchain technology.* Georgetown McDonough School of Business Research Paper No. 3131250.

Biswas, S., & Sen, J. (2016). A proposed architecture for big data driven supply chain analytics. *International Journal of Supply Chain Management, 13*(3), 7–34.

Brindley, C. (2004). *Supply Chain Risk*. Williton, VT: Ashgate.

Butner, K. (2010). The smarter supply chain of the future. *Strategy & Leadership, 38*(1), 22–31.

Delen, D., & Demirkan, H. (2013). Data, information and analytics as services. *Decision Support Systems, 55*(1), 359–363.

Evans, J. R. (2012). Business analytics: the next frontier for decision sciences. *Decision Line, 43*(2), 4–6.

Güller, M., Koc, E., Hegmanns, T., Henke, M., & Noche, B. (2015). A simulation-based decision support framework for real-time supply chain risk management. *International Journal of Advanced Logistics, 4*(1), 17–26.

Henke, M. (2009). *Supply risk management: Planung, Steuerung und Überwachung von Supply Chains*. Berlin: Erich Schmidt Verlag.

Henke, M., Blome, C., Seifert, M., Grötsch, V., & Sauerbier, M. (2010). *Intensives Risikomanagement oder flexibles Krisenmanagement? Überlebensstrategien im Automobileinkauf in der Wirtschaftskrise.* Wiesbaden: Supply Chain Management Institute (SMI).

Jüttner, U., Peck, H., & Christopher, M. (2003). Supply chain risk management: Outlining an agenda for future research. *International Journal of Logistics: Research and Applications, 6*(4), 197–210.

Khan, O., & Zsidisin, G. A. (2012). *Handbook for supply chain risk management: Case studies, effective practices and emerging trends*. Fort Lauderdale, FL: J. Ross Publishing.

Mitchell, V. W. (1995). Organizational risk perception and reduction: A literature review. *British Journal of Management, 6*(2), 115–133.

Norrman, A., & Jansson, U. (2004). Ericsson's proactive supply chain risk management approach after a serious sub-supplier accident. *International journal of physical distribution & logistics management, 34*(5), 434–456.

Pettit, T. J., Fiksel, J., & Croxton, K. L. (2010). Ensuring supply chain resilience: Development of a conceptual framework. *Journal of Business Logistics, 31*(1), 1–21.

Raab, M., & Griffin-Cryan, B. (2011). *Digital transformation of supply chains*. White Paper: Capgemini Consulting.

Rozados, I. V., & Tjahjono, B. (2014). Big data analytics in supply chain management: Trends and related research. In *6th International Conference on Operations and Supply Chain Management*, Bali.

Sanders, N. R. (2014). *Big data driven supply chain management. A framework for implementing analytics and turning information into intelligence*. Upper Saddle River, NJ: Pearson Education.

Satyavolu, P., & Sangamnerkar, A. (2016). Blockchain's smart contracts: Driving the next wave of innovation across manufacturing value chains. In *Cognizant 20–20 Insights*, June.

Schrauf, S., & Bertram, P. (2017). Industry 4.0: How digitization makes the supply chain more efficient, agile, and customer-focused. *Price Waterhouse Coopers Strategy*.

Seuring, S., & Müller, M. (2008). From a literature review to a conceptual framework for sustainable supply chain management. *Journal of Cleaner Production, 16,* 1699–1710.

Sodhi, M. S., & Tang, C. S. (2012). *Managing supply chain risk (International Series in Operations Research & Management Science)*. New York: Springer.

Svensson, G. (2000). A conceptual framework for the analysis of vulnerability in supply chains. *International Journal of Physical Distribution & Logistics Management, 30*(9), 731–750.

Svensson, G. (2002). Dyadic vulnerability in companies' inbound and outbound logistics flows. *International Journal of Logistics and Research Applications, 5*(1), 13–44.

Tang, C. S. (2006). Perspectives in supply chain risk management. *International Journal of Production Economics, 103*(2), 451–488.

Tummala, R., & Schoenherr, T. (2011). Assessing and managing risks using the supply chain risk management process (SCRMP). *Supply Chain Management: An International Journal, 16*(6), 474–483.

Wang, G., Gunasekaran, A., Ngai, E. W. T., & Papadopoulos, T. (2016). Big data analytics in logistics and supply chain management. Certain investigations for research and applications. *International Journal of Production Economics, 176,* 98–110.

Wu, T., & Blackhurst, J. V. (2009). *Managing supply chain risk and vulnerability: Tools and methods for supply chain decision makers*. Berlin: Springer Science & Business Media.

Yoo, S. (2017). Blockchain based financial case analysis and its implications. *Asia Pacific Journal of Innovation and Entrepreneurship, 11*(3), 312–321.

Yu, M.-C., & Goh, M. (2014). A multi-objective approach to supply chain visibility and risk. *European Journal of Operational Research, 233*(1), 125–130.

Zsidisin, G. A. (2003). Managerial perceptions of supply risk. *Journal of Supply Chain Management, 39*(1), 14–25.

Zsidisin, G. A., & Ellram, L. M. (2003). An agency theory investigation of supply risk management. *Journal of Supply Chain Management, 39*(3), 15–27.

Zsidisin, G. A., Ellram, L. M., Carter, J. R., & Cavinato, J. L. (2004). An analysis of supply risk assessment techniques. *International Journal of Physical Distribution & Logistics Management, 34*(5), 397–413.

Zsidisin, G. A., Panelli, A., & Upton, R. (2000). Purchasing organization involvement in risk assessments, contingency plans, and risk management: An exploratory study. *Supply Chain Management: An International Journal, 5*(4), 187–197.

Zsidisin, G. A., & Ritchie, R. (2009). *Supply chain risk: A handbook of assessment, management & performance*. New York, NY: Springer International.

Part I
Assessing Supply Chain Risk—The First Step in Managing Supply Chain Risk

Chapter 2
Assessing the Vulnerability of Supply Chains: Advances from Engineering Systems

Sigurd S. Pettersen and Bjørn Egil Asbjørnslett

1 Introduction

1.1 Background

Modern, global supply chains are characterized by complex networked structures. Companies interact to produce complex products through manufacturing processes that rely on thousands of suppliers in multiple layers with limited knowledge of each other. As supply chains are becoming longer and more complex, resulting from changes in the global marketplace, companies become vulnerable to disruptions at seemingly peripheral nodes. Minor incidents spiral out of control, exposing weaknesses beyond those captured by traditional risk analyses. Hence, there is a need for vulnerability assessments that consider a wider set of threats and weaknesses, as well as the resources to recover supply chain functioning.

Over the last twenty years, there has been an immense growth in literature that documents vulnerability assessments for supply chains (Asbjørnslett and Rausand 1999; Peck 2005; Svensson 2000). This literature has grown to include the application of methodology from system safety (Adhitya et al. 2009; Asbjørnslett 2009; Berle et al. 2011a, b). Recently, there has also been a strong trend toward including socio-technical aspects more strongly in system design, connecting the design, management, and operation of increasingly complex engineering systems. Engineering systems have been characterized as engineered systems with a high degree of social and economic intricacy, meaning that these systems are partially designed, and partially evolve through their use (de Weck et al. 2011). This is similar to the view of

S. S. Pettersen (✉) · B. E. Asbjørnslett
Norwegian University of Science and Technology (NTNU), Trondheim, Norway
e-mail: sigurd.pettersen@ntnu.no

B. E. Asbjørnslett
e-mail: bjorn.e.asbjornslett@ntnu.no

G. A. Zsidisin and M. Henke (eds.), *Revisiting Supply Chain Risk*, Springer Series in Supply Chain Management 7, https://doi.org/10.1007/978-3-030-03813-7_2

supply chains as complex adaptive systems (Choi et al. 2001), which cannot merely be seen as designed systems as they continuously evolve. Together, these trends have led to the development of tools that may be valuable additions to the toolbox available to supply chain practitioners and researchers. For thorough reviews on the recent advances on methodologies for supply chain risk management, we refer to Tang and Musa (2011) and Heckmann et al. (2015).

Tools from engineering systems, including reliability engineering, system dynamics, and operations research, have significantly improved the state of, and opportunities for, vulnerability assessment in supply chains. Still, a number of promising concepts and perspectives that have been influential in the design of engineering systems deserve to be introduced to the supply chain context as these have potential to improve the state of vulnerability assessment.

1.2 Objectives

The main objective of this chapter is to update a generic framework for supply chain vulnerability assessment with tools that have been developed for the design and management of engineering systems. This chapter introduces tools that originate from systems engineering and engineering design into the supply chain risk management context. The authors believe that these recommended tools and methods from the engineering systems domain will inspire practitioners and academics interested in supply chain management to apply them, hence improving on the practice of vulnerability assessment in supply chain risk management.

2 Concepts and Definitions

This section describes the fundamental terms that are needed to understand vulnerability assessment in supply chains as covered in previous work (Asbjørnslett 2009). Concepts and definitions relating directly to the advances we introduce later in the chapter are given in Sect. 4.

Vulnerability describes the characteristics of a supply chain that weakens or limits its abilities to withstand threats originating inside or outside the supply chain system boundaries (Asbjørnslett 2009). The vulnerability can be manifested in any of the constituent systems in the supply chain, and in supply chain processes, operation, and management. The constituent systems can be divided into nodes; production facilities, warehouses, ports, terminals, and so on, and transportation modes flowing between the nodes; road, rail, waterborne, and airborne. The supply chain system is subjected to the expectation that it should be able to meet societal as well as business demands, while being vulnerable to a wide array of threats, like technical failure, human error, loss of personnel, accidents, hostilities from malevolent agents, natural disasters, volatility in demand and energy prices, and so on. Hence, we define

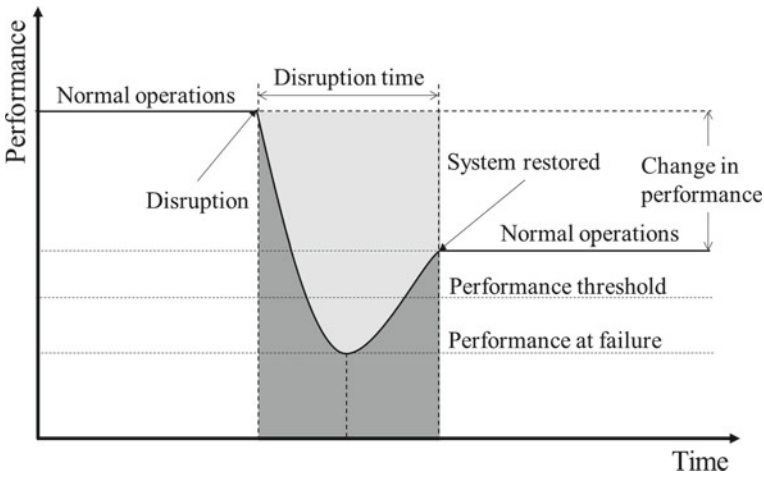


Fig. 1 Performance profile for a resilient system (Asbjørnslett and Rausand 1999)

vulnerability, following Asbjørnslett (2009), as "the properties of a supply chain system that may weaken or limit its ability to endure threats and survive accidental events that originate both within and outside the system boundaries."

In contrast to vulnerability, we also define resilience and robustness. These concepts describe the characteristic behavior of the supply chain system when meeting a disruption. Resilience is defined as the ability of the system to recover from a disruption, whereas robustness is the ability to resist the effects of a disruption (Asbjørnslett 2009). The concepts can be further differentiated by an analogy to material science. Whereas resilience describes the elastic deformation of a material, a robust system would be resistant to perturbations that generate elastic deformations, but may experience a completely brittle failure if the load is increased.

Figure 1 shows the performance profile for a resilient system over time. From an initial level of "normal operations," the performance drops due to a disruption to a minimum given by "performance at failure." The performance after recovery needs to exceed a "performance threshold" for minimal acceptable performance. Accordingly, resilience becomes a function of the "disruption time," and the "change in performance." In contingency planning for system recovery, these dimensions of resilience need to be assessed relative to costs (Pettersen et al. 2018).

3 Framework for Vulnerability Assessment

This section introduces the fundamental framework for vulnerability assessment that was presented by Asbjørnslett (2009). Vulnerability assessments should be understood as an extension in comparison to the scope of a risk assessment. Risk assess-

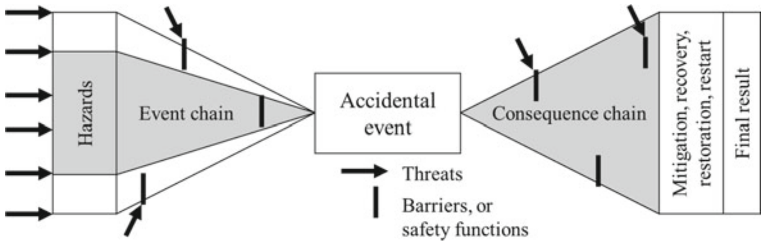


Fig. 2 An extended bow-tie model that accounts for vulnerability assessment

ments seek to answer what can go wrong, and answer what the consequences and likelihood of these scenarios are (Kaplan and Garrick 1981). Vulnerability assessments extend this scope to identify an extended set of threats and consequences, identify adequate resources for mitigation, recovery and restoration of the system, while taking into consideration the disruption time before a new stable state is found (Asbjørnslett 2009). Figure 2 illustrates the scope of vulnerability assessments in a bow-tie model, in comparison to a risk assessment.

The framework for vulnerability assessment presented by Asbjørnslett (2009) aims to:

- Provide insight into the threat and risk picture of the given supply chain in its context, and develop a taxonomy of system characteristics contributing to vulnerability.
- Analyze scenarios of how vulnerabilities evolve, and rank the scenarios according to criticality, within the relevant supply chain management context.
- Enable decision-making regarding acceptance of vulnerabilities by assessing alternative strategies for reducing the likelihood or consequences of analyzed scenarios.

The framework consists of the following seven steps, which are briefly explained here. See Asbjørnslett (2009) for a more comprehensive run-through.

1. **Definition of scope of work**:
   We define the frame and targets for analysis. This includes setting the objectives, determining the unit of analysis, and setting the system boundaries. An important element of this is to determine acceptance criteria for vulnerabilities.
2. **Description of SC/SCM context**:
   We describe the context within which the supply chain system operates. A generic description of context will capture all exogenous factors that have the ability to influence the supply chain performance.
3. **Taxonomy development**:
   We develop a structured set of vulnerabilities pertaining to the supply chain context defined earlier. Setting up a taxonomy of factors that influence vulnerability allows efficient collection of relevant knowledge for further analysis.

4. **Scenario development**:
   We develop scenarios starting from the threats identified in the earlier steps of the analysis, considering a scenario as a sequence of events through the bow-tie in Fig. 2, until the system is in a stable, disrupted state. Hence, the scenario does not include the actions taken to mitigate, restore, recover, or restart.
5. **Criticality ranking**:
   We rank the scenarios in accordance with their criticality, which in a risk assessment we normally calculate as the product of likelihood and consequence (Rausand 2011). In a vulnerability assessment, we need to extend the criticality estimate to include the availability of resources we can use to bring the system back to a new stable level of performance.
6. **Scenarios of importance**:
   We visualize the output of the criticality assessment so far by plotting the scenarios in a risk (likelihood/consequence) diagram with consequences on the x-axis and likelihood along the y-axis. The effect of actions to mitigate, recover, restore, or restart can also be plotted in the diagram.
7. **Reducing likelihood and consequence**:
   We consider implementations of measures to reduce likelihood, or to reduce the consequences of the scenarios, on the basis of the previous steps. More emphasis has typically to be put on the reduction of likelihood, even though this should not overshadow preparation to deal with consequences.

4 An Updated Toolbox

The tools presented herein fulfill three overall purposes in the context of vulnerability assessment. First, epoch-era analysis can be applied to create contextual awareness by enabling evaluation of supply chain performance in a wide set of circumstances that evolve through time. Second, "failure mode thinking" focuses the treatment of specific accident scenarios on the impact on functionality, implying that consequences are more important to get right than the probabilities of the accidental event in vulnerability assessments. Third, methods from systems design are employed to enhance the understanding of whether system components can cover a failure mode, caused by loss of functionality in some other system components.

Figure 3 illustrates the role of these tools in relation to the framework for vulnerability assessment. The outer layer in the figure points out that epoch-era analysis provides structure to the context definition. The intermediate layer points out that failure mode thinking will enable a focus on loss of functionality as the primary method of vulnerability identification. The inner layer shows that the functional view of vulnerabilities enables engineering design tools that map between function and form to identify ways that functionality can be covered when failure modes are encountered.

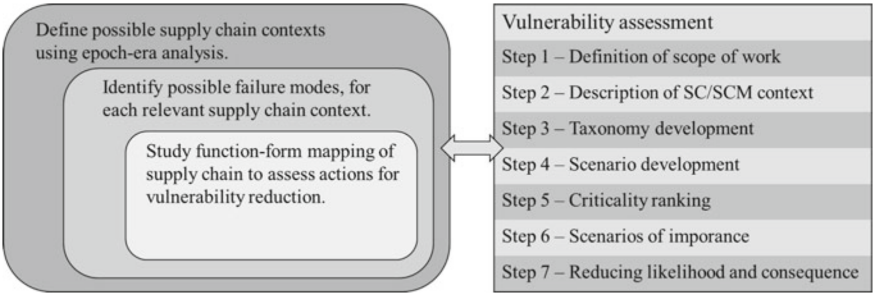


Fig. 3 New tools for vulnerability assessment

4.1 Epoch-Era Analysis

Epoch-era analysis (EEA) is a technique from the systems engineering community, first introduced by Ross and Rhodes (2008), which was developed for analyzing the value of a system through its life cycle. This method is often coupled with multi-attribute tradespace exploration (MATE) models (Ross et al. 2004) to represent system value for all possible system configurations, but it can also be applied independently from MATE. The primary use of EEA has been in the lifecycle assessment of complex engineered systems, which are subject to considerable future uncertainty with respect to context, and stakeholder needs. In this respect, it is a decision support tool for system design. However, EEA can also be used to structure scenarios by modeling and sequencing static contexts for existing systems, like supply chains. Note that, in the EEA framework, a scenario refers to the evolution of system context through time, and not necessarily the causal chain of events in the bow-tie model.

We define an “epoch” as a time period described by a static system context, and static stakeholder needs. For systems in general, and supply chains in particular, it is important to consider at this stage where the system boundaries lie. Is our unit of analysis the supply chain or a focal company operating within a supply chain? If we take the view that we study the whole supply chain using EEA, we consider perturbations that stem from the context of the supply chain. On the other hand, if we study the focal company within a supply chain, the supply chain becomes the context. Studying changes in supplier and customer relations and then becomes relevant to the analysis.

We describe every contextual factor that is to enter into the EEA as an epoch variable. The epoch variables are normally discrete variables that can take on values that span the range of possible outcomes. A vector of epoch variables then describes an epoch. Depending on the number of contextual factors taken into account as epoch variables, and the fidelity chosen for these, the number of possible epochs explodes. As the epoch describes a static context and needs combination, it represents the concept known in economics as the short run where all production parameters remain fixed (Ross and Rhodes 2008). This means that epochs can serve as the basic building blocks for dynamic, long-run scenarios.

We define an “era” as any sequence of epochs in time, hence representative of the dynamic, long-run scenario describing the evolution of context. Hence, the era concept can be a way to frame a narrative some stakeholders think is a likely future scenario. When describing future scenarios through telling a story, stakeholders may include contextual background information whose impact on system value is very difficult to quantify. For example, if a scenario is to be used to inform a decision regarding buying a car, a detailed recount of the situation in the Middle East is not directly relevant, even though this situation may impact the price of gasoline, which in turn influences what car should be bought. Rather, the decision maker could go directly to using historical gas prices as input to the EEA model, rather than speculating about global politics. Hence, structuring narratives using the era concept, the redundant dimensions of the narrative can be reduced, so that the model only contains the exogenous factors that affect value directly.

Methods for era generation range from purely qualitative approaches, using narratives to determine which epochs to use as basic building blocks, to probabilistic methods, using simulation to generate eras from the epochs. Probabilistic methods rely on rules that eliminate eras that are illogical, for example, by taking into account that certain contextual changes are irreversible. If we study a focal company within a supply chain, and the supplier goes bankrupt, this is often an irreversible change in context. Hence, the bankrupted supplier cannot emerge in a later epoch.

Figure 4 shows how a set of illustrative epoch variables can be structured on the basis of a set of more generic exogenous factors whose direct influence on the supply chain performance are more difficult to understand, and hence left out of the analysis. The system dynamics that underlie the background exogenous factors are complex. Instead of describing scenarios using these, we settle on describing scenarios from the direct factors that have an influence on a company within the supply chain, hence encapsulating complexity. The EEA therefore serves as a scenario-structuring mechanism that can be useful in vulnerability assessment.

The main advantages of using EEA can hence be summarized as follows:

- EEA enables structured thinking about the current context and possible future contexts by encapsulating complexity behind the well-defined epoch vector interface.
- EEA enables structured thinking about the evolution of scenarios in the long run, by sequencing well-defined epochs in a reasonable manner.

4.2 Failure Mode Methods

The word “failure mode” is derived from the reliability engineering domain, where it refers to the loss of functionality in a component (Rausand and Høyland 2004). When experiencing a failure mode, the component no longer delivers the desired output. This concept has been widely used in reliability engineering, as part of the method-

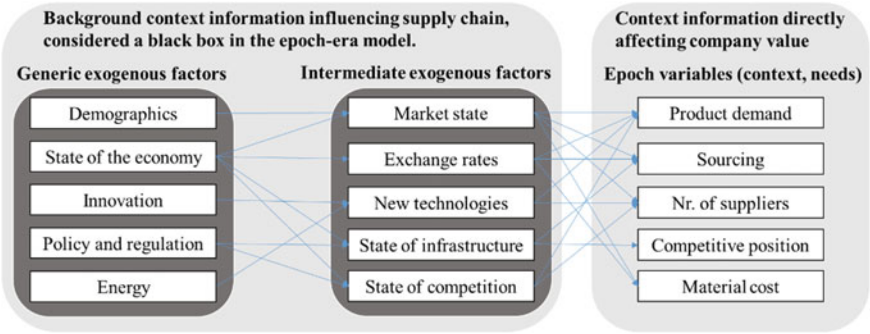


Fig. 4 Mapping from a set of indirect factors (black box) to a set of epoch variables that directly affect company value. The examples are meant to be illustrative only

ology called failure modes, effects, and criticality analysis (FMECA) (Rausand and Høyland 2004). This methodology supports decisions regarding conceptual system design, development, and operation by determining whether designs are sufficiently reliable (sufficiently low probability of operational disruption). The outcomes of such analysis are regularly used in quantitative risk assessment, where the product of likelihood and consequence guides whether additional risk reducing measures should be implemented. In reliability engineering, decisions at this stage relate to whether it is cost-efficient to add redundancies.

In a supply chain context, failure modes can be understood as a way in which one element of the supply chain losses its ability to fulfill its function in the supply chain. With reference to the supply chain operations reference (SCOR) model (Supply Chain Council 2012), this can be a failure to fulfill any subfunction to the five main functions; to plan, source, make, deliver, or return the product. Hence, a functional decomposition of these functions will provide additional insight into the reasons why the supply chain fails to function normally, without speculating about the exact chain of events. Figure 5 relates the SCOR model with the functional structure and location of potential critical failure modes.

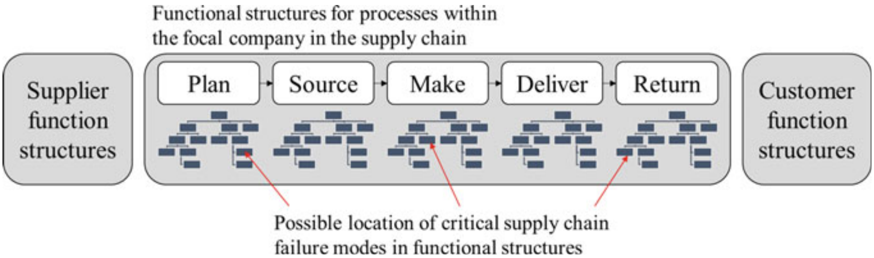


Fig. 5 Relating supply chain operations reference model with functional structures for failure mode identification

Berle et al. (2011a) use the failure mode concept to identify vulnerabilities in maritime supply chains. Their argument is that methods that focus on each scenario simplify the difficulties in foreseeing the causal chain leading to the supply chain losing functionality. Very infrequent events that deserve proper attention due to severe consequences are not sufficiently addressed when risk is defined as the product of likelihood and consequence. By devising an approach to vulnerability assessment which mainly seeks to identify how functionality can be lost, supply chain managers can turn to develop a business continuity plan for each failure mode. Naturally, business continuity planning should seek to restore functionality at reasonably high levels of fidelity in the functional hierarchy. In other words, to the focal company in Fig. 4, the best path forward from a disruption is not necessarily to restore the activity at the component that previously experienced a failure. Rather, the company should seek to cope with the failure mode by shifting its operations to components that retain the ability to function.

Starting from the failure mode perspective, Berle et al. (2011b) base their approach to vulnerability assessment in maritime transportation on the formal safety assessment (FSA) framework developed by the International Maritime Organization (International Maritime Organization 2002). Berle et al. (2011a) propose that two distinct procedures for safety assessment can be followed, based on the degree to which risks can be foreseen. Even if we acknowledge that not all risks are known, we know what functions the system consists of, and hence failure mode consequences can be taken into account. The proposed framework presents two parallel tracks. A hazard-focused procedure is used for the known risks, while a mission-focused procedure is suggested for the "unknown" risks where the failure mode approach offers the most insight into what capabilities are lost. The framework used by Berle et al. (2011b) is presented in Table 1 for illustrative purposes only.

Table 1 Formal vulnerability assessment with a mission-based focus making use of failure modes (Berle et al. 2011)

	FVA description	Hazard focus	Mission focus
Step 1	Hazard identification	What may go wrong?	Which functions should be protected?
Step 2	Vulnerability assessment	Investigate/quantify most important risks	Investigate/quantify most important failure modes
Step 3	Vulnerability mitigation	Measures to mitigate most important risks	Measures to restore functions/capabilities
Step 4	Cost/benefit assessment	Cost/benefit assessment	
Step 5	Recommendations for decision-making	Recommendations and feedback	

4.3 System Design Methods

4.3.1 Engineering Design Methodology

While supply chains have the characteristics of complex adaptive systems that are subject to emergent behaviors as well as control (Choi et al. 2001), we will see that there are certain advantages of applying the methods of engineering design in supply chain risk management. For example, we can consider the supply chain system as a partially designed and partially evolved "physical" system that meets a set of functional requirements, for example, the generic processes outlined by the SCOR model referenced earlier.

System design is a process of developing descriptions of physical systems that can provide the functions necessary to meet some need. This is often referred to as mapping between function and form. Axiomatic design (Suh 1990) and catalogue design (Pahl and Beitz 1996) are two commonly referred design methodologies. Suh (1990) proposes two fundamental design axioms to establish guidelines for the design process. First, the independence axiom states that functional requirements (FRs) should be kept independent, by mapping one-to-one onto design parameters (DPs) in the form space. Second, the information axiom states that the amount of information contained in a system should be kept minimal. Applications of these principles imply a less complex system, which will be less prone to fail in unexpected ways, and easier to control. These principles are not necessarily something we wish to follow when it comes to supply chains, as these systems are not purely objects of design. Still, they are useful for illustrating how function maps onto form. Axiomatic design often makes use of design matrices that illustrate how the functional requirements are met by a physical description represented by design parameters. An example of the uncoupled design, which is the most desirable state in accordance with axiomatic design, is shown in Eq. (1).

$$\begin{Bmatrix} FR_1 \\ FR_2 \end{Bmatrix} = \begin{bmatrix} a_{11} & 0 \\ 0 & a_{22} \end{bmatrix} \begin{Bmatrix} DP_1 \\ DP_2 \end{Bmatrix} \tag{1}$$

The reliance on design matrices is similar to the use of design structure matrices for visualization of complex project development processes (Steward 1981), that has also been applied to managing the function–form mapping in system design (Eppinger and Browning 2012). Common applications of design structure matrices include sequencing of processes in project management and clustering analyses to modularize product architectures by encapsulating components performing related functions within modules in accordance with axiomatic design principles.

Pahl and Beitz (1996) suggest that design processes should consist of task clarification, conceptual design, embodiment design, and detail design. Once desired functionalities are defined through the task clarification, and the conceptual design process can commence by developing functional structures and using design catalogues to find physical solutions that can provide the physical effects meeting the

Table 2 Notional design catalogue for use in function–form mapping for the supply chain

Classifying criteria	Solutions	Solution characteristics	Remarks
Supply chain processes, and functional hierarchies (see Fig. 5.)	Firms within supply chain, and organizational structure of firms that can solve functions	Explanation of how the solutions map onto the classifying criteria	Additional information needed
	Further alternatives …	…	…

desired functionality. Finding a solution then becomes a question of combining the solutions that are found from the catalogue into a design that meets the overall needs. Design catalogues enable quick, problem-oriented access to proven solution principles for the functions, and often contain accumulated knowledge from earlier design processes. A notional design catalogue for use in a supply chain risk management setting is shown in Table 2.

The literature referenced above signifies that the mapping between function and form is essential in system design. However, it does not distinguish sufficiently between those capabilities that a designed system is intended to have, and those that it actually possesses. Axiomatic design points to the intentional function–form mapping using design matrices that map between these domains, while catalogue design provides a comprehensive guide to alternative solutions for meeting these functions so that designers can combine solutions in the synthesis.

4.3.2 Considering Latent Functions and Functional Redundancies

The understanding that complex systems can produce behaviors and provide functionality exceeding what was expected is also found in the social sciences. Merton (1968) describes latent functions as the functions that are neither intended nor recognized, as opposed to manifest functions which are intended and recognized. The primary purpose of this framework is to analyze the effects of policy, understanding that social planning has unforeseen consequences. Latent functions have been discussed in the context of functional modeling for complex engineering systems by Crilly (2010) who points out that the functionality that carries a value, depends on the context, the stakeholders, and evolves through time. Crilly (2015) points to the need for viewing system functioning both in relation with the supersystem in which the system is a part, and in relation to the context the system works in. Pettersen et al. (2018) show that exploiting latent capabilities benefits resilience, while breaking with the design axioms of Suh (1990). They suggest how latent capabilities can be identified and implemented into the function–form mapping to enable recovery from a failure mode. The manifest functions, and the latent functions are distinguished in Fig. 6, where latent functions are activated to recover from the failure mode. Recovery is here enabled by latent capabilities, as DP_2 has the ability, without intent or

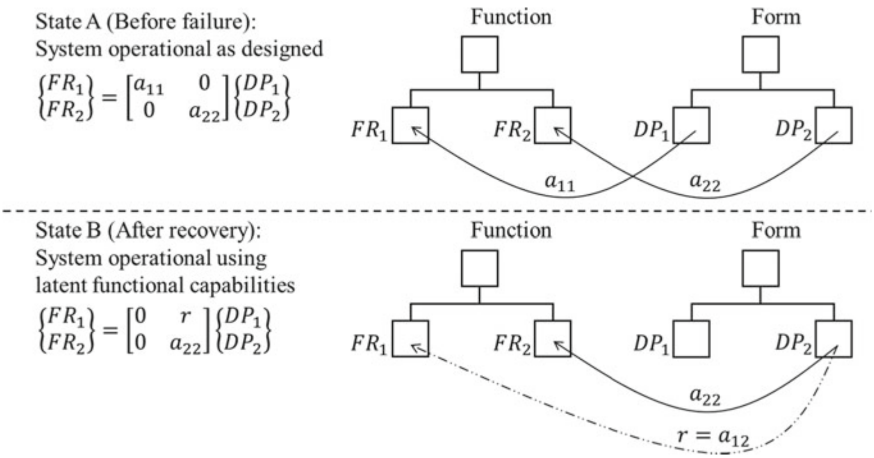


Fig. 6 Functional and physical system structures. State A indicates system as designed. State B indicates system operational using latent capabilities (Pettersen et al. 2018)

recognition during design, to perform FR_1. An advantage of applying latent capabilities compared with other means to recover is that we utilize existing resources in a new way, and hence, functionality can be restored swiftly.

Erden et al. (2008) review functional modeling in the system design and artificial intelligence literature and state that when meeting disruptions due to failure, "another component, rather than the faulty one, can perform the function, perhaps in a less efficient way." They point to the similarity of this concept to that of functional redundancy, which is commonly cited as a design principle to achieve system resilience (Jackson and Ferris 2013; Rice Jr. and Caniato 2003; Uday and Marais 2015). The main difference is perhaps that functional redundancies are something that are designed with intent, while latent capabilities emerge from observed behaviors that were not thought of beforehand. Functional redundancies are favored over physical redundancies, based on adding redundant components to the design, as it does not change the "physical form" of the system, and does not come at an additional investment cost (Erden et al. 2008; Jackson and Ferris 2013). In supply chain systems that evolve outside the control of a single stakeholder, system components will likely possess latent functions that can be taken advantage of to reduce the impact of disruption. We now show how these capabilities can be exploited to reduce vulnerability.

The following example differentiates what the system *is intended to do*, from what the system *can do*: Consider a situation where Team A has been assigned to Process A, while Team B has been assigned to Process B. However, if both teams are able to perform both tasks, the intended function–form mapping derived through a design synthesis does not capture all capabilities. An additional step of *analysis* may be needed to understand the full spectrum of capabilities, after the design process.

Intended capabilities

Functional structure (FRs) / Physical structure (DPs)

	Team A	Team B
Process A	1	0
Process B	0	1

All (intended and unintended) capabilities

Functional structure (FRs) / Physical structure (DPs)

	Team A	Team B
Process A	1	1
Process B	1	1

Fig. 7 Comparing the intended capabilities (left) of a system as assigned, with the complete available capabilities (right) of the system

The resulting differences between the intended organizational capabilities and the overall potential capabilities of the same organization are shown in Fig. 7.

Hence, capabilities beyond the intended can be taken advantage of, for example to provide functional redundancy, should hazards materialize and cause functional failure in the supply chain. We consider the example of a supply chain which can be described as a mapping between function and form, as shown in Fig. 8. Here, a set of functional requirements $\{FR_A, FR_B, FR_C, FR_D, FR_E\}$ is to be met. We accept that the supply chain is a complex adaptive system, and hence, it does not adhere to the design axioms. We then investigate whether DP_B can meet any other function, finding that it can meet FR_E. If we have access to a design catalogue that describes every solution that can be used to provide FR_E, we find that one such solution is DP_B. Due to this, DP_B can provide functional redundancy should DP_E fail to meet FR_E.

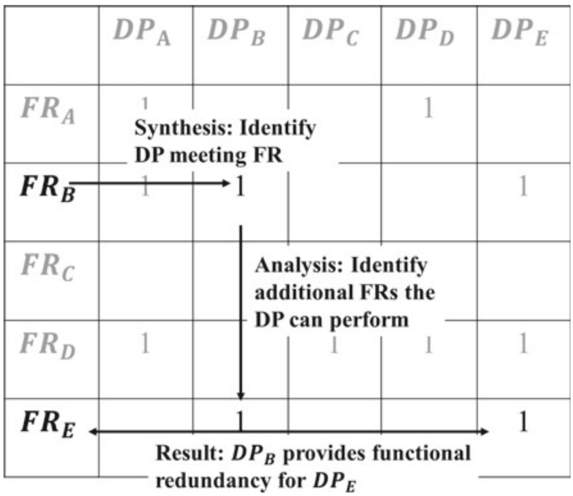


Fig. 8 Identifying functional capabilities beyond the intended (latent functions)

5 Using the Toolbox in Supply Chain Vulnerability Assessment

This section presents a more thorough description of each step in the vulnerability assessment briefly introduced in Sect. 3, with emphasis on how the toolbox introduced in Sect. 4 can be applied in the vulnerability assessment. Figure 9 connects the worksheets used in vulnerability assessment with the toolbox presented in Sect. 4.

5.1 Step 1: Definition of Scope of Work

The initial step of the assessment defines the frames and targets of analysis. It is important to scope the analysis consistently, for the vulnerability assessment to proceed with the appropriate amount of rigor and with a reasonable structure. In this initial phase, it is also important to assign sufficient resources and time to the analysis, and ensure that a multi-disciplinary team is involved, that are able to elicit important information from all relevant supply chain stakeholders. We can distinguish four elements that need to be properly assessed in Step 1:

1. **Determine objectives for the analysis**
   What do we want to find out? Why do we want to know what?
2. **Determine the unit of analysis**
   What elements of the supply chain do we analyze?
3. **Determine system boundaries**
   What is inside the system boundaries? What exogenous factors affect the system directly?
4. **Determine vulnerability acceptance criteria**
   What are acceptable levels of vulnerability after actions are taken?

The second and third points listed are particularly important with respect to the additional tools we propose. Setting the system boundaries, we should think through

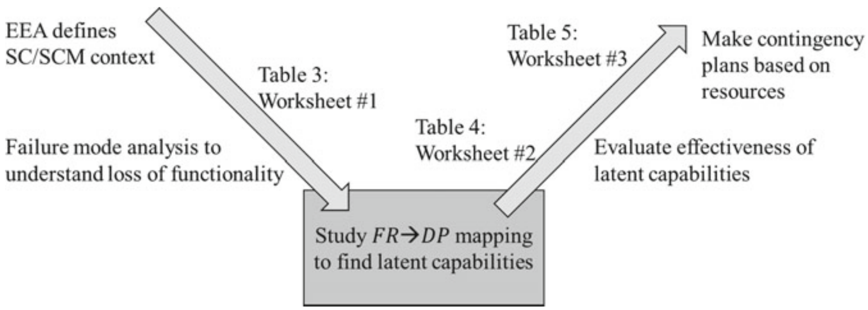


Fig. 9 Toolbox set in context with central worksheets for the vulnerability assessment framework

what aspects of the problem can be controlled, and what exogenous factors directly influence the supply chain. These aspects will strongly frame the remaining steps of the vulnerability assessment.

5.2 Step 2: Description of SC/SCM Context

The second step addresses the impact of the supply chain context, as indicated by Step 1. For supply chain systems that continuously adapt by including new supplier and customer relations with other rational agents, we should not consider context as something static. Instead, sets of contexts can be developed and sequenced as long-run dynamic contexts. Epoch-era analysis proposes that we parameterize context variables that are subject to uncertainty. Then we can make a model that maps the influence of the context onto system vulnerability. Hence, we can obtain an understanding of how the risk picture will look for every context developed, by constructing epochs. Further, by stringing together epochs into eras, we can infer possible evolution of vulnerabilities facing long-term supply chain operations.

To describe the supply chain context using epoch-era analysis, we elicit a preliminary set of uncertainties and develop the relationship between supply chain vulnerability, value, and the context factors. There is a need for verification that the chosen context factors have a quantifiable impact on the supply chain. Generic factors that will affect the supply chain context include the supply/demand situation, the strength of competitors, the relationship to customers and suppliers, and the cost structure. Depending on the context, different sets of vulnerabilities may be interesting to investigate further. Tools that can complement epoch-era analysis in framing the supply chain context, include Kraljic's classification taxonomy for supply (Kraljic 1983) and Porter's five-force analysis (Porter 1979). Notice that when we frame the supply chain context in a particular way, we may lose out on some perspectives. A solution to this problem can be to work with a large number of contexts, possibly developed in parallel by several teams of analysts, even though this reduction in reliance on specific assumptions would come at the cost of an increased workload.

A major implication of using epoch-era analysis to frame the context of the supply chain is that we need to treat the remainder of the steps as context-dependent. Hence, for every alternative representation of the supply chain context, we should go through Steps 3–7.

5.3 Step 3: Taxonomy Development

While Step 2 proposes that we develop context sets via epoch-era analysis, this step establishes a structured set of context-dependent vulnerabilities. The structured set of vulnerabilities will be used to develop the scenarios in Step 4. As we can understand the supply chain system in terms of the functionality delivered by its nodes, the failure mode approach referred to in Sect. 4.2 can be useful. Vulnerabilities can be entered into the taxonomy based on their impact on the functional hierarchy that can be developed for the system as suggested by the formal vulnerability assessment introduced by Berle et al. (2011b), or by using a number of alternative taxonomies outlined by Asbjørnslett (2009). This enables a focus on determining which functions should be protected, rather than understanding the scenarios, and hence, the analysis is more strongly geared toward enabling continued or restored functioning.

5.4 Step 4: Scenario Development

The fourth step is to develop scenarios. We define scenarios as sequences of possible events that are separated in space and time, originating from an accidental event, and where barriers that should prevent the sequence are included. The starting point is one of the elements identified in the taxonomy in Step 3, upon which a sequence of events until a stable, disrupted state can be imagined. The scenario itself then does not include any efforts to mitigate or recover from the disrupted state. A variety of risk management methods exist that have had influence on scenario development for accidental events. See Rausand (2011) for a comprehensive overview of accident models and scenario building methods.

At the closure of Step 4, a sufficient amount of knowledge has been collected to document the scenarios. Table 3 represents a notional worksheet for documentation. In the first column (i), the outcomes of Step 3, given its contextual dependency on Steps 1 and 2, are provided. For every relevant supply chain context, this represents a checklist for the factors that should be covered through the analysis. In the second column (ii), the scenarios are described, as suggested in Step 4. The sequencing of events, proceeding through proactive and reactive barriers, allows the analysts to determine whether or not this sequence is likely to disrupt the supply chain functioning. The preliminary answer to whether a scenario is likely to have this effect is entered into the third column (iii), in order to limit the amount of information to consider in the later steps. If the analysts perceive the scenario as a possible threat to supply chain survival, they will enter the failure mode that disrupts the supply chain in the fourth column (iv). At this point, we have an overview of the causal links between an initiating event and loss of functionality, which enables the system analysts to assess the possible recovery options. These options are documented in the fifth and sixth columns (v–vi), ranked according to whether there is a use of internal (v) or external (vi) resources for recovery. The system design methods introduced in Sect. 4.3 are particularly applicable for this, as these largely focus on the understanding of how functions can be achieved through the behaviors of a physical system. Design catalogues often contain many alternative proven solutions to how a lost function can be recovered. As mentioned, the resources needed to recover from disruption may already exist somewhere in the supply chain. There is only a question about uncovering where and what supply chain components possess latent function-

Table 3 Worksheet #1; documentation of scenarios (Asbjørnslett 2009), with examples of possible methods that can be used

Threat (i)	Scenario (ii)	Likely (yes/no?) (iii)	Potential immediate effects? (iv)	Resources/systems/plans for mitigation, restoration, rebuilding, etc.		Remarks (vii)
				Internal (v)	External (vi)	
Given by current context (EEA)			Which function is disturbed?	Identify latent capabilities using design catalogues, to restore function.		

Table 4 Worksheet #2; criticality ranking of scenarios (Asbjørnslett 2009)

Scenario description	Likelihood of scenario (i)	Consequences of scenario			Resources to mitigate, recover, restore…		Total critical-ity (vii)
		Service (ii)	Costs (iii)	'Other' (iv)	Internal (v)	External (vi)	
1		Assessment of failure modes			Evaluate effectiveness of resources (latent capabilities)		
2							
…							

ality. We refer to Pettersen et al. (2018) for a discussion of how latent capabilities can be utilized. Column (vii) makes detailed remarks, if further details are needed.

5.5 Step 5: Criticality Ranking

The fifth step quantifies the criticality associated with every scenario developed within the alternative contexts in the previous steps. The purpose is to assess the likelihood and consequences associated with each of the scenarios. Table 4 suggests a structured worksheet for this part of the analysis. First, a likelihood score for every scenario is set (i). Then, the consequences with respect to a set of different factors are established, and scored, including the impact on the quality of service delivered (ii), the costs accrued (iii), and "other" (iv), which may include the duration of disruption, loss of reputation, and so on. Thereafter, the ease with which resources to mitigate and recover from the accident is scored. The scoring of such resources can be justified by considering that functionality can more easily be restored if there are latent capabilities in the system, than if the system needs to be reconfigured through additional investments or repair. The total criticality is given in the seventh column (vii), often calculated as the product of the likelihood and the consequences.

5.6 Step 6: Scenarios of Importance

The sixth step makes use of risk matrices to create an understanding of which scenarios are the most important to address for possible system contexts. A risk matrix ranks the scenarios according to the consequence and likelihood, as exemplified in Fig. 10. In the figure, scenarios that were found in Step 5 are ranked in accordance with their consequence and likelihood, placing the scenarios in relation to criticality. Darker shade here indicates higher criticality.

Naturally, based on the risk matrix in Fig. 10, it is important to attend to the scenarios of higher criticality and emphasize particularly those scenarios that are very critical, with no known recourse to mitigation, restoration, or rebuilding resources. Measures to reduce the consequences are shown as arrows. For example, we can consider Scenario 2 and Scenario 4. We see that both these fall within the "high critical" area. An important difference is that some consequence-reducing measures have been identified for Scenario 2, while none such measures exists for Scenario 4. This means that Scenario 4 should be prioritized before addressing Scenario 2. Determining scenarios of importance thereby results in a list of prioritized scenarios to follow up on, either to understand the causal links leading up to scenarios to enable prevention of causes and interactions, or to improve impact reducing measures.

5.7 Step 7: Reducing Likelihood and Consequence

The final step of the framework establishes how actions can be made to reduce the likelihood and consequences of the scenarios and focuses on vulnerability reduction through decision-making on the levels of supply chain design and operation. Table 5 shows a worksheet example for this step.

Normally, it is desirable to avoid disruptions altogether, hence first, we should consider means to avoid or reduce the threats (i), and means to reduce the probability of accidental events (ii). Next, measures to reduce consequences should be introduced. These include designing passive barriers into the supply chain (iii), like redundancies and margins. Redundant functionality can be found by using design catalogues. Further, we consider measures related to operations and active barriers (iv). Last, we seek means for mitigating, restoring, and rebuilding the supply chain capabilities after the scenario has materialized (v). For the measures to reduce conse-

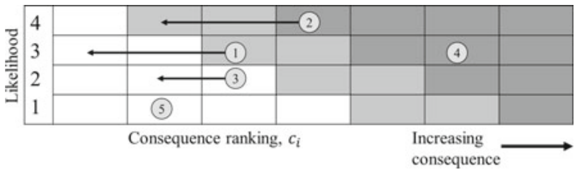


Fig. 10 Risk matrix representation for the scenarios of importance (Asbjørnslett 2009)

Table 5 Worksheet #3; evaluating measures with potential to reduce likelihood and consequence (Asbjørnslett 2009)

Scenario description	Reduction of likelihood		Reduction of consequences		
	Measures to avoid or reduce threats (i)	Measures to reduce the probability of accidental events (ii)	Measures related to design and passive barriers (iii)	Measures related to operations and active barriers (iv)	Measures related to mitigation (v)
1			Contingency planning relying on latent capabilities to recover from failure modes		
2					
…			Alternative means …		

quences, there is room for basing contingency plans on measures that involve latent capabilities.

6 Summary

This chapter has introduced a number of novel tools for use in vulnerability assessment for supply chains. The presented tools originate in research fields unfamiliar to most practitioners and researchers of supply chain management. These tools have been set into the context of a framework for vulnerability assessment presented in an earlier chapter (Asbjørnslett 2009). The main advantages of applying the new tools are:

- An improved understanding of how alternative context and needs affect supply chain vulnerability through epoch-era analysis.
- An improved understanding of how functional modeling via the failure mode approach can be used to address low-frequency, high-impact supply chain disruptions.
- An introduction to the latent capabilities concept enables identification of new ways to restore lost functionality. We suggest that latent functions are identified by the use of design catalogues.

We believe that the use of these methods will improve supply chain resilience and provide a competitive advantage to firms that learn to consciously apply these concepts and tools in their supply chain management philosophy.

References

Adhitya, A., Srinivasan, R., & Karimi, I. A. (2009). Supply chain risk identification using a HAZOP-based approach. *AIChE Journal, 55*(6), 1447–1463.

Asbjørnslett, B. E. (2009). Assessing the vulnerability of supply chains. In G. A. Zsidisin & B. Ritchie (Eds.), *Supply chain risk—A handbook of assessment, management, and performance* (pp. 15–33). New York, NY: Springer Science+Business Media.

Asbjørnslett, B. E., & Rausand, M. (1999). Assess the vulnerability of your production system. *Production Planning & Control, 10*(3), 219–229.

Berle, Ø., Rice, J. B., Jr., & Asbjørnslett, B. E. (2011a). Failure modes in the maritime transportation system: a functional approach to throughput vulnerability. *Maritime Policy & Management, 38*(6), 605–632.

Berle, Ø., Asbjørnslett, B. E., & Rice, J. B., Jr. (2011b). Formal vulnerability assessment of a maritime transportation system. *Reliability Engineering and System Safety, 96*(6), 696–705.

Choi, T. Y., Dooley, K. J., & Rungtusanatham, M. (2001). Supply networks and complex adaptive systems: control versus emergence. *Journal of Operations Management, 19,* 351–366.

Crilly, N. (2010). The roles that artefacts play: Technical, social and aesthetic functions. *Design Studies, 31*(4), 311–344.

Crilly, N. (2015). The proliferation of functions: Multiple systems playing multiple roles in multiple supersystems. *Artificial Intelligence for Engineering Design, Analysis and Manufacturing, 29,* 83–92.

de Weck, O. L., Roos, D., & Magee, C. L. (2011). *Engineering systems: Meeting human needs in a complex technological world*. Cambridge, MA: The MIT Press.

Eppinger, S. D., & Browning, T. R. (2012). *Design structure matrix: Methods and applications*. Cambridge, MA: The MIT Press.

Erden, M. S., Komoto, H., van Beek, T. J., D'Amelio, V., Echavarria, E., & Tomiyama, T. (2008). A review of function modeling: Approaches and applications. *Artificial Intelligence for Engineering Design, Analysis and Manufacturing, 22*(2), 147–169.

Heckmann, I., Comes, T., & Nickel, S. (2015). A critical review on supply chain risk—Definition, measure and modeling. *Omega, 52,* 119–132.

International Maritime Organization (2002). Guidelines for Formal Safety Assessment for use in the IMO rule-making process. London, UK.

Jackson, S., & Ferris, T. L. J. (2013). Resilience principles for engineered systems. *Systems Engineering, 16*(2), 152–164.

Kaplan, S., & Garrick, J. B. (1981). On the quantitative definition of risk. *Risk Analysis, 1*(1), 11–27.

Kraljic, P. (1983). Purchasing must become supply management a strategy for supply. *Harvard Business Review*, 109–117.

Merton, R. K. (1968). *Social theory and social structure*. New York, NY: Macmillan Publishing Co.

Pahl, G., & Beitz, W. (1996). *Engineering design* (2nd ed.). London, UK: Springer.

Peck, H. (2005). Drivers of supply chain vulnerability: An integrated framework. *International Journal of Physical Distribution & Logistics Management, 35*(3/4), 210–232.

Pettersen, S. S., Erikstad, S. O., & Asbjørnslett, B. E. (2018). Exploiting latent functional capabilities for resilience in design of engineering systems. *Research in Engineering Design, 29*(4), 605–619.

Porter, M. E. (1979). How competitive forces shape strategy. *Harvard Business Review, March–April*, 137–145.

Rausand, M. (2011). *Risk assessment: Theory, methods, and applications* (1st ed.). Hoboken, NJ: John Wiley & Sons Inc.

Rausand, M., & Høyland, A. (2004). *System reliability theory: Models, statistical methods and applications* (2nd ed.). Hoboken, NJ: Wiley.

Rice, J. B., Jr., & Caniato, F. (2003). Building a secure and resilient supply network. *Supply Chain Management Review, 7*(5), 22–30.

Ross, A. M., Hastings, D. E., Warmkessel, J. M., & Diller, N. P. (2004). Multi-attribute tradespace exploration as front end for effective space system design. *Journal of Spacecraft and Rockets, 41*(1), 20–28.

Ross, A. M., & Rhodes, D. H. (2008). Using natural value-centric time scales for conceptualizing system timelines through epoch-era analysis. In: *INCOSE International Symposium* (Vol. 18, pp. 1186–1201). Utrecht, The Netherlands.

Steward, D. V. (1981). The design structure system: A method for managing the design of complex systems. *IEEE Transactions on Engineering Management*, *EM-28*(3), 71–74.

Suh, N. P. (1990). *The principles of design*. New York, NY: Oxford University Press.

Supply Chain Council. (2012). *Supply chain operations reference model* (11th ed.).

Svensson, G. (2000). A conceptual framework for the analysis of vulnerability in supply chains. *International Journal of Physical Distribution & Logistics Management, 30*(9), 731–750.

Tang, O., & Musa, S. N. (2011). Identifying risk issues and research advancements in supply chain risk management. *International Journal of Production Economics, 133*(1), 25–34.

Uday, P., & Marais, K. (2015). Designing resilient systems-of-systems: A survey of metrics, methods, and challenges. *Systems Engineering, 18*(5), 491–510.

Chapter 3
Using Scenario Planning to Supplement Supply Chain Risk Assessments

Cliff Thomas and Thomas Chermack

1 Introducing a Well-Known Problem

Much has been written about the increasing complexity of supply chains and the risks associated with them, and supply chain managers are likely to observe that risk factors have become greater in number and more complicated. It is not uncommon for organizations to involve hundreds, or even thousands of suppliers. In these conditions, the implications for risk management are staggering, as the vast assortment of an organization's internal risk concerns are more or less replicated in each supply chain partner: operational risk, regulatory risk, financial risk, employee risk, technology risk, and others. In essence, organizations can exponentially increase their own level of risk through creating a critical dependence on risk-exposed suppliers.

Consequently, in the contemporary environment's level of risk, complexity, and turbulence, supply chain managers face unprecedented levels of uncertainty (Chermack 2011). In this chapter, we acknowledge these realities, adopting the perspective that the physical, logistical, and technological systems associated with supply chain risk management (SCRM) have become more complicated, are exposed to more failure points, and are largely outside of the customer's control.

In the face of such circumstances, what are supply chain risk managers to do? Pragmatically, they do what they can. They extinguish the daily fires associated with supply chain glitches, they stay in tune with likely problems, and they implement strategies to mitigate the most probable sources of harm. In a perfect world, such sources would be certain. But in this world, we are reminded by Albert Einstein's

C. Thomas (✉)
Risk Management Consultant, Atlas Group, Inc. 217 W. Olive Street,
Fort Collins, CO 80521, USA
e-mail: cliff@atlasprep.com

T. Chermack
Scenario Planning Institute, Colorado State University, Fort Collins, USA
e-mail: Thomas.Chermack@colostate.edu

G. A. Zsidisin and M. Henke (eds.), *Revisiting Supply Chain Risk*, Springer Series in Supply Chain Management 7, https://doi.org/10.1007/978-3-030-03813-7_3

sentiment that "realistically, nothing is certain; and what is certain is not realistic." All too often, however, managers and leaders follow a different path.

1.1 Attempting to Make the Uncertain, Well … Certain

Milliken (1987) described uncertainty as the perceived inability to accurately predict something. Naturally, events can be more or less certain. The result of a coin flip is 50% uncertain. The roll of two dice landing on 7 is about 83% uncertain. But in the context of supply chain risk, how uncertain is a building fire at a critical supplier's facility? Or the bankruptcy of a key supplier? Or a critical supply chain technology failure? For complex organizations, such a list might seem endless, and the uncertainty of each concern could defy quantification. Despite these realities, organizations still must take action to manage supply chain risk.

Often, risk management strategies and operational controls are outgrowths of a supply chain risk assessment. The general risk assessment process typically involves five steps: (1) risk identification, (2) risk assessment and evaluation, (3) risk management strategy selection, (4) strategy implementation, and (5) contingency and risk mitigation planning. Out of this process, the managers and leaders seek to answer three questions: "of the threats we've identified, which events are most likely to occur?", "what are the consequences of those events?", and "what can we do to lessen harmful consequences?".

While different supply chain managers generally have similar risk management aims, they tend to adopt different approaches to achieve them: those of *probabilistic choice* or *risk analysis* (Miranda and Proenca 1997, 1998). *Probabilistic choice* is based on the cumulative average of possible outcomes associated with an event. For example, if an event of interest relates to a supplier's adherence to quality standards, the calculation would involve the number of units delivered and the range of quality measures associated with each unit. In this example, the average value of the data set becomes the proxy for the most probable future. Probabilistic choice has validity for repetitive events for which ample data is available, but it does not account for outlier events such as natural disasters or other catastrophic situations. For these types of events, past events can be a deceptive guide to the future.

In comparison, *risk analyses* focus on the difference between the actual cost of an adopted solution, as compared to the cost of an optimal solution made with knowledge of future events. This difference is occasionally represented as "regret." In this case, the decision-maker adopts a more costly or less costly solution based on harm associated with potential future outcomes. As an example, a supply chain risk manager who spends $100,000 to mitigate a particular risk would likely be less "regretful" than if she had spent $500,000 to more fully mitigate that risk, assuming the risk was never realized. In risk analyses, decisions are obviously made without knowledge of future events, so managers must hedge their bets by weighing the costs of solutions against potential consequences. Ultimately, though, each manager makes a decision that reflects a particular version of the future.

Our main point in describing common risk assessment paradigms is that both are designed to answer the question "what do we think will happen?" Managers and leaders must pick their own versions of the future in order to develop coherent supply chain risk mitigation measures. This is entirely reasonable. However, we suggest that the task of risk assessment is not complete at this point. Other possibilities for harm still exist, and managers would be wise to be sensitive to them. We propose scenario planning as a practical and effective method by which organizations can educate and sensitize decision-makers about a range of futures, what they portend, and how their emergence might be recognized.

1.2 A Gap in Research

Although scenario planning research has been frequently applied within the domain of supply chain risk management, we argue that the research has largely been solution-focused, and therefore has not examined the expansive nature of scenario planning envisioned by Schwartz (1996), Wack (1985), and others. For valid reasons, supply chain risk researchers have often asked questions akin to: "given a wide range of risks, what can practitioners do to manage them?" Results have yielded various methods and strategies: what-if analyses, event tree analyses, multi-sourcing, inventory buffers, and many others. While these outcomes are pragmatic and address practitioners' immediate needs, the research orientation toward an optimal solution fosters reductionist thinking that does not account for supply chain risk's inherent uncertainty. We suggest an alternative research question that leads to expansive thinking: "given that practitioners can only manage a portion of their risk, what *else* should they be attuned to?" In a world in which problems are complex and uncertain, such an awareness can be powerful.

2 Scenario Planning: Accepting Uncertainty

> [Under uncertainty] there is no scientific basis on which to form any calculable probability whatever. We simply do not know. Nevertheless, the necessity for action and for decision compels us as practical men to do our best to overlook this awkward fact (…).
>
> —John Maynard Keynes (1937)

2.1 Plausible Futures, not Forecasts

As compared to probabilistic choice and risk analysis, scenario planning offers a fundamentally different risk assessment paradigm by posing the questions "what future states could emerge, what might these futures entail, and how can we recognize them in their early stages?" Scenario planning accepts the reality that decision-makers are not equipped with a crystal ball and forecasts and projections are destined to fail at some point. It also suggests that if the actual future deviates from the forecasted future, knowledge about the emerging situation will be highly beneficial to decision-makers.

2.2 A Divergence from Other Scenario Planning Methods

While the term "scenario planning" is frequently used within the supply chain risk profession, such techniques often involve practices more accurately described as "what-if analyses" and "event tree analyses." In these methods, scenarios relate to the cascading effects of a known failure events. These methods are generally not intended to imagine plausible futures that emerge based on driving forces, but to guide the selection of risk management solutions.

The scenario planning approach proposed in this article is markedly different from these approaches. First, scenario planning does not focus on whether a particular risk event will happen or not. Rather, it centers on various *driving forces* that could influence future risks to the organization, and a description of what those futures might look like. Second, the goal of scenario planning is not to arrive at "a solution." In fact, selecting a particular risk management solution is more akin to forecasting and is antithetical to the scenario planning process. The goal of scenario planning is to engage decision-makers in meaningful dialogue that fosters understanding of central issues that are critical to the future of the organization, and to broaden their perceptions about the types and natures of situations that could emerge.

At its core, scenario planning fosters creative thinking, insights into plausible futures, improved decision-making, enhanced organizational learning, and imagination (Chermack 2011). In doing so, the practice elevates managers' knowledge about their environments, widens their perceptions of possible future events, and enables better decision-making (Schwartz 1996). As Schoemaker et al. (2013) have suggested, managers tend to focus on immediate problems and concerns, effectively blinding them to peripheral indicators that catastrophe could be looming. It is our contention that being sensitive to such indicators is a necessary component of supply chain risk management, and that scenario planning is an effective way to develop risk sensitivity.

3 The Roots of Scenario Planning

The origins of contemporary scenario planning are frequently attributed to the pioneering work of Herman Kahn, Pierre Wack, and other visionaries of the 1950s and 1960s. Kahn's scenario-building approach contributed to paradigmatic shifts in US military and civil defense strategies. Through research that was unconstrained by military assumptions, Kahn observed that US strategy was based on wishful thinking more so than reasonable expectations. The term "thinking the unthinkable" was coined as a result of Kahn's work (Bradfield et al. 2005), a term that continues to resonate in today's environment.

Along with others at Royal Dutch/Shell (Shell), Wack built on Kahn's work to engage 15-year "horizon planning" for the company as the 1960s came to a close. For Shell, horizon planning was undertaken to provide the company with insights into plausible ranges of future oil demands, which would in turn have implications for production and pricing. At that time, oil company-based production on long-term demand forecasts and set their own prices. Because of market stability, demand forecasts tended to adopt the same assumptions year after year, yielding a relatively straight-line trajectory "up and to the right." Consequently, production and pricing also were considered to be very predictable.

Departing from the norms of demand forecasting, Wack spent considerable time examining the implications of severe price shocks and other market forces. He was able to see clearly how Shell's regression lines and predictive approaches to resource allocation were failing year after year. When OPEC took control of oil pricing and initiated the 1973 embargo, Shell found itself as the only major oil company to have taken measures to weather just such an event. During this period of sky-rocketing oil demand, the company quickly recognized the signs of the oil crisis and its implications. As a result, "having talked together about the problem, the executives were at least reasonably well prepared to weather the crisis" (Kleiner 2008, p. 152). Fundamentally, Wack believed that in order to analyze future scenarios, managers must recognize that forecasts are fallible, and must understand the forces that influence the systems of their businesses (Wack 1985).

Based on the work of Kahn, Wack, and others, the concept of scenario planning has evolved into a method used to explore a wide range of complex problems with unknown solutions (Chermack 2011, 2017). Modern-day scenario planning has spanned across the industry landscape, focusing on problems ranging from food supply chain security to geopolitical influences on the airline industry (Moyer 1996). While "classic" risk analysis continues as a way to manage "what we think will happen," scenario planning provides a compelling approach to addressing "what we didn't know could happen."

4 Using Scenario Planning for Supply Chain Risk Management

> The future is here. It is just not widely distributed yet—Author William Ford Gibson

Scenario planning is often a group process involving a series of interactive workshop sessions that can occur over a series of days, weeks, or months, depending on the nature of the topic being considered. The number of participants involved in workshops can range from a handful to a large group—again, based on the aims of the process. Over the course of the workshops, participants engage in dialogue that produces insights about uncertain situations and how those can affect the organization.

The design of the scenario planning process helps managers overcome mental anchors that can fixate their thinking on the present and the recent past. Further, the intentionally broad range of perspectives helps organizations overcome groupthink behaviors that produce homogeneous thinking year after year. Unique to the scenario planning method is that the process and the outcome are somewhat equivalent: The aim is to engage decision-makers in thoughtful and imaginative discussions about "what could happen" over a time horizon of interest. The range of futures that could happen has been described as an uncertainty cone, a broader perspective than the "forecasted future," as depicted in Fig. 1 (adapted from Schoemaker et al. 2013, p. 818). Within the uncertainty cone, it is seen that decisions might fall within official forecasts, but it is also possible that they will not.

In considering futures that have not been officially forecasted, managers are armed with knowledge and insights about a wide range of situations that they might not have otherwise considered. From a supply chain standpoint, we suggest that this knowledge could put managers in a better position to make decisions about the need for alternate suppliers, safety stock, inventory storage locations, supplier audits, contractual obligations, and other risk control measures.

4.1 Involving the Right People

The composition of the scenario planning team should enable the exploration of new paradigms, and therefore calls for diverse perspectives and backgrounds. For some organizations, it will be tempting to merely engage an existing management team in the scenario planning process. Before taking this step, it is worthwhile considering whether an established team can break out of deep-rooted group norms, behaviors, and expectations. Maybe, or maybe not. And if not, will the process generate new understandings?

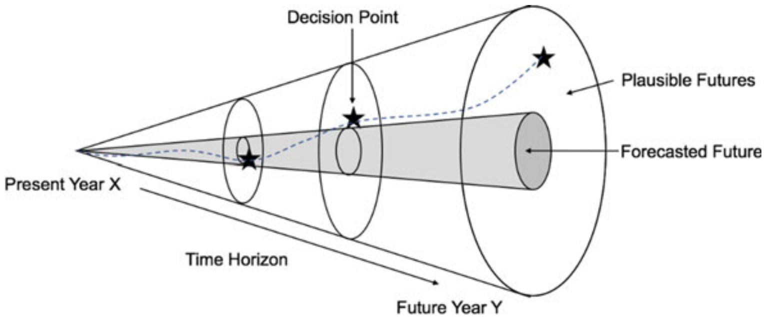


Fig. 1 Uncertainty cone

We suggest the deliberate engagement of new voices and perspectives as a way to yield new and meaningful insights. For the purposes of supply chain risk, organizations might consider engaging participants serving in supervisory, management, and executive levels. Cross-functional disciplines might include supply chain planning, logistics, warehouse operations, purchasing, and other related disciplines. Wack even took this practice to inviting total outsiders to the scenario processes—he called them "remarkable people" (Chermack 2017).

Furthermore, because supply chain management relies on a range of interdependent business functions, those perspectives should also be considered. We have often found that organizations typically have a vast wealth of knowledge and skills, but they frequently reside in silos and are not fully utilized. The practice of "connecting dots" within organizations—engaging people in settings that promote information sharing—can be among the most powerful tools available for managing risk. When thinking about scenario planning for supply chain risk, we propose consideration be given to business functions external to the organization's supply chain department:

- *Finance* can provide insights regarding long-range supply chain management budgets.
- *Regulatory Affairs* is often able to provide information about supplier licensing in other countries, the regulatory implications of disruptions, and the nature of changing regulatory requirements in various regions. This is particularly true of global supply chains which operate in unstable regions of the world.
- *Information Technologies* can provide insights into the organization's overall IT resilience and vulnerability to cyber-attacks, the consequences of various IT disruptions, and the realities of new supply chain partner technology integration.
- *Legal/Contracting* can provide insights into legal and contractual implications of supply chain disruptions, as well as contractual obstacles related to alternate or new suppliers.
- *Enterprise Risk Management* has likely thought about key risks to the organization and may also have a keen understanding of Board of Director risk concerns. These risks might have direct implications for SCRM.
- *Business Development, and Research and Development* are often able to help paint a picture of what a firm's future product and service profile might look like, in turn driving supply chain requirements and priorities.
- *Corporate Services* such as Security and Human Resources often have vast knowledge about internal and external influences on SCRM.

4.2 The Focusing Question

Having formed the project team, it is important that the members be engaged in all subsequent activities. The team should be involved in directing the project; a process quite different than the project manager-centric approach, in which team members are assigned designated tasks to execute. As a first step in establishing the direction of the scenario planning project, the team engages in dialogue to identify the problem or the decision of interest: typically in the form of a focusing question. For strategic planning, the focusing question might look 5–10 years in the future. Operational questions will likely consider a shorter time horizon, perhaps 6 months to 3 years. The nature of the specific business and industry will inform those timelines.

The focusing questions form the foundation of all following scenario planning activities, so the importance of this step should not be minimized. A vague or uninspiring question will likely lead to similar outcomes. This is another reason why the scenario planning team's engagement is essential: The members should have some passion for the question being posed, suggesting that later in the process the team will dedicate energy to scenario development. Below are examples of various focusing questions related to supply chain risk strategy and operations. Note that some questions range in specificity, as determined by each organization's unique set of concerns.

"How will our global supply chain risk profile change over the next 10 years?"

"How will the opening of a South American market affect our supply chain risk over the next 5 years?"

"In what ways will cyber-threats impact our supply chain over the next 3 years?"

"How can government changes in our South America market impact our supply chain over the next 3 years?"

In selecting a focusing question, the scenario planning team will likely enter into spirited discussion. But, to reiterate, this is the point: interaction and learning. Even if the process stopped at this point, individuals representing a range of business functions would have gained an appreciation for SCRM concerns that may have been new to them.

4.3 Brainstorming Influences on the Focusing Question

Once the project team has settled on a focusing question, the team then identifies the driving forces that have an influence on the focusing question. This process begins with the brainstorming of issues that each team member believes are important with respect to the focusing question. To get a full range of responses, it is often helpful if members are prompted to consider STEEP impacts—social, technical, economic, environmental, and political (Chermack 2011). Depending on the nature of the focusing question, other impact contexts might be appropriate for consideration. The context of PESTLE may be appropriate if legal matters are also of concern, and the STEEPLE context is appropriate to further account for ethical concerns. For example, within the STEEP context, if the focusing question is "What will affect the supply chain in our US market over the next 5 years?" A team member might list issues listed below (the reader can surmise what the consequences related to each issue might be):

Social influences

- Potential for organized labor strikes at our European port
- Staffing shortages at warehouse locations
- Consumer activism affecting our industry

Technical influences

- Power system reliability
- Cyber-intrusion into our supply chain management system
- Telecommunication disruptions

Economic influences

- Fuel cost swings
- US inflation
- Changes in corporate tax rates

Environmental influences

- Market supply and demand fluctuations
- Industry contraction/expansion
- New competition in our US market

Political influences

- Changes in NAFTA
- Administrative requirements related to Asian imports/exports
- More stringent business licensing standards in South America

Above we have provided examples of three issues under each STEEP category. In reality, a scenario planning team is likely to generate a few hundred issues of concern. Attempting to cope with this number of issues is both unrealistic and unnecessary. Therefore, next we will discuss how the scenario planning team can effectively manage such large quantities of data.

4.4 Grouping Individual Forces into Driving Forces

Individual issues of concern are unlikely to drive strategic change, and many will be limited to specific contexts, as illustrated in the examples above. But viewed in the aggregate, they comprise broader categories are apt to provide a more meaningful and expansive context for scenario building. Moreover, it is likely that many of the brainstormed concerns are either duplicative or related in some way. For both of these reasons, individual concerns must be consolidated into more comprehensive driving force categories. For example, concerns related to "power system reliability," "telecommunications disruptions" and "water quality" might be designated as a category designated as "Critical Infrastructure." The driving force of Critical Infrastructure is therefore described by all of its associated underlying concerns.

As with other activities in the scenario planning process, this is a task for the scenario planning team to complete. By creating and naming the categories of driving forces, the team members will participate in rich and informative discussion about a wide range of supply chain risk issues, and why people view them as being important. As mentioned earlier, it is often flashes of insight that are generated from these discussions that form new “mental anchors” that influence peoples’ future actions and decision-making.

4.5 Ranking and Rating Forces

Once the driving forces have been identified, the team is charged with assigning each category with *impacts rankings* and *uncertainty ratings*. The team first ranks the categories based on the extent to which the category could impact the focusing question. Typically, this process does not occur in an orderly sequence. Rather, perspectives about implications of each category tend to adjust throughout the process as the team members become more informed about the implications of each driving force. The ranking process is illustrated in Fig. 2a, b. The outcome is simply the ordering of driving forces from least impactful to most impactful.

Once driving forces are ranked by impact, the team will rate each category by its level of certainty. Again, this is usually not accomplished sequentially, and robust dialogue provides all team members with meaningful insights into problems they

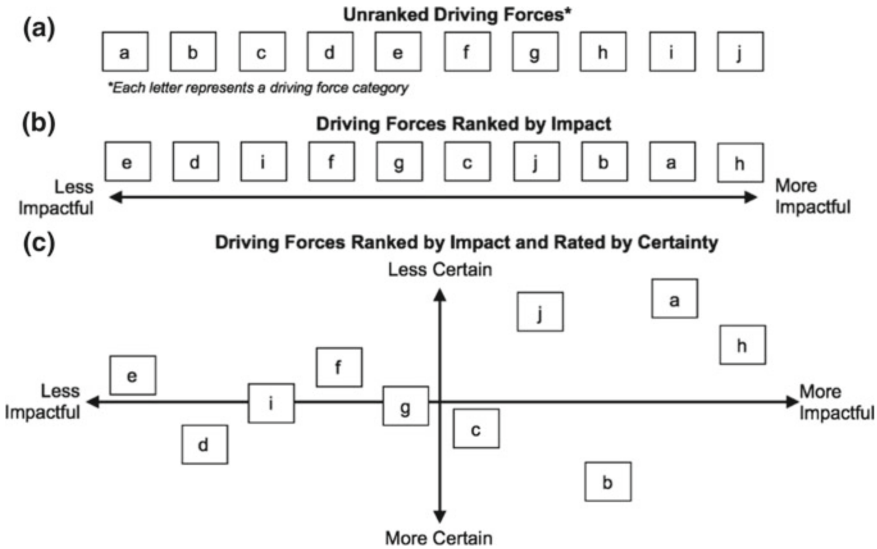


Fig. 2 Driving force rating and ranking steps

may not have recognized. Figure 2c shows an example of the outcome of the rating and ranking process.

Risk management professionals will note that this approach is fundamentally different from the classic formula "*risk* = *probability* × *impact*". A weakness inherent in this formula is that both "probability" and "impact" are often assigned values based on weak or flawed support, derived with little internal dialogue (Hubbard 2009). As a result, the approach can generate numeric outcomes which can be misleading and only superficially understood. Scenario planning, on the other hand, acknowledges the uncertainty of future events, and through dialogue, seeks to develop a deeper level of understanding about their implications.

4.6 The Scenario Matrix

The team is now ready to focus on a particular set of forces that will drive scenario development. To do this, the team decides which two categories serve as interesting and compelling issues. The categories need not be related to each other, but typically, categories of interest will have been ranked and rated as highly impactful and highly uncertain. In other words, these are the plausible futures that the team might understand very little about, but that could cause substantial harm.

Once the two driving forces of interest are identified, they are situated on a 2 × 2 matrix in which each axis represents a range of potential future states. To illustrate, we will draw from a 2017 study analyzing current supply chain risks. In this study, the top two emerging threats of concern were identified as (a) cyber-security and (b) new laws and regulations (BCI 2017). When thinking about the range of possibilities for the driving force "cyber-security," one end of the axis might reflect a technological status quo, and the other might represent the introduction of new technologies and new associated threats. The axes do not necessarily represent conditions that are necessarily "good vs. bad"; rather, they represent alternative states—a "this versus that" dichotomy. As with previous tasks, team member discussion is needed to complete this step. For instance, the example matrix in Fig. 3 reflects driving forces concerning laws and regulations, and cyber-threats.

4.7 Writing Scenarios

Using the completed 2 × 2 matrix, the scenario planning team has identified four types of futures that reflect varying combinations of driving forces. The goal in this step is to create a plausible description of a future associated with each combination of categories. That process begins by first envisioning the essence of each matrix quadrant—this might be thought of as developing various narratives of future states. Using the example shown in Fig. 3, the scenario planning team might develop the following types of narratives:

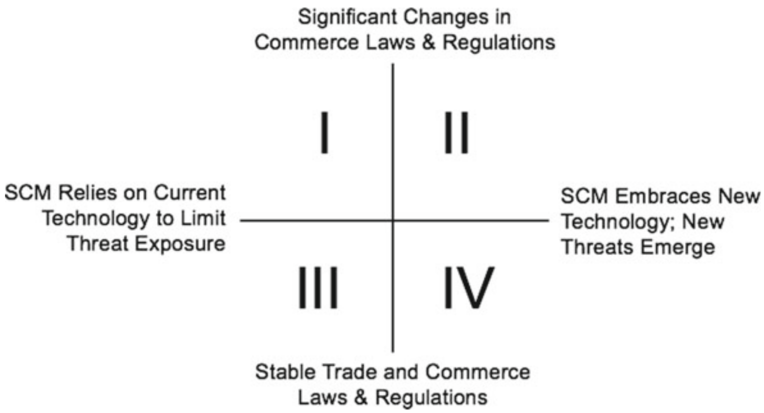


Fig. 3 Example scenario matrix

Quadrant I—This future envisions a state in which existing supply chain technology must be adapted to meet the demands of new laws and regulations.
Quadrant II—In this future, supply chains contend with a chaotic environment in which both new cyber-risks and new standards create an ongoing scramble to achieve security and compliance.
Quadrant III—This quadrant describes a future in which supply chain managers rely on current technology, and relevant laws and regulations remain largely unchanged.
Quadrant IV—In this future, supply chain managers adopt new technological solutions that present a novel and changing cyber-threat landscape.

While merely creating narratives for each future can be challenging, writing a rich and descriptive story for each quadrant is scenario planning's heavy lifting: It requires the entire team's imagination and persistence. Thinking about possibilities can be an abstract process, often uncomfortable to those whose daily responsibilities revolve around concrete performance measures. Fortunately, the scenario planning process provides ample material to support the creation of each story: Not only will each driving force be underpinned by many issues identified during the brainstorming sessions, but the dialogue which occurred throughout the process will have given team members a higher level of appreciation for the implications of the driving forces.

With the narrative as a guide, the team engages in creating an account that, to the extent possible, incorporates the issues that underlie each driving force. There are no shortcuts in this step of the process; nor should there be. By engaging with each other on what various plausible futures could look like, the participants will have armed themselves with a level of awareness and understanding of supply chain risks that had likely not been forecasted. Ultimately, stories should flesh out rich descriptions of future states that represent each quadrant of the driving forces matrix. The stories should "bring the futures" to life in a way that resonates with all scenario planning team members. Ideally, these will be stories that form mental anchors in the team members, providing them with insights that could be critical, depending on the future that emerges.

4.8 An Alternative to the Scenario Matrix Approach

It should be emphasized that scenario planning was not always codified in the steps described above. In fact, when Wack started out using scenarios at Shell in the 1960s his process was much more fluid. Wack did not believe there was any set of steps that could be followed to achieve useful and effective scenarios (Chermack 2017). Instead, he deliberately formed a team of deep thinkers. A key criterion for inclusion on his team was evidence of a way of thinking contrary to Wack's own. It was common for Wack to recruit people with significantly different ethnic, political, and cultural backgrounds. This ensured a lot of different ways of seeing the world were involved, as well as a lot of arguing. Wack and his team would spend weeks at offsite locations, commonly without phones or televisions, and focus on leveraging their diverse expertise to shed new light on an issue. Instead of following steps, they muddled through until some key varied themes emerged.

Years after Wack retired from Shell, others decided to codify the scenario process into steps, guidelines, and frameworks that make using scenarios easier than having a resident "mystic." Today, the most common approach to scenario planning is indeed the matrix approach; however, highly creative teams need only the goal of developing some provocative storylines around important risks.

4.9 Identifying Signals for Action

Once developed, scenarios can enable the early recognition of signs that various plausible futures are emerging, allowing organizations to take early action. As with Pierre Wack and Royal Dutch/Shell, the fact that decision-makers had become familiar with an unexpected future enabled them to communicate more effectively and initiate actions earlier than if they had been engaged in trying to understand what was happening. In order to identify signals and related actions, Chermack (2011) suggests holding workshops specifically designed to achieve those aims. In the first workshop, the team identifies early warning signals by considering the following question: "How will we know that (driving force) is starting to occur?" Once those thoughts are collected and synthesized, another workshop is held to focus on the question: "If we detect (this signal), what can we do about it?" Schoemaker et al. (2013) propose that the periodic examination of risk through multiple scenario perspectives signals is an effective means of keeping a "signals library" current, as well as the resulting actions that have been identified.

5 Scenario Planning Challenges

Scenario planning is energizing, enjoyable, and rewarding. It enlightens decision-makers about issues they likely would not have considered, and may not have recognized if they had come to pass. We propose that it is an appropriate technique in analyzing complex and uncertain risks associated with supply chains. On the other hand, its distinctive approach can deviate from contemporary organizational norms and practices. Managers and leaders can struggle with the idea that scenario planning may not produce a decision or solution. In today's hyper-focus on efficiency, performance, and outcomes, this can be unsettling. And as a result, participants can fall back into well-established paradigms that drive toward a single solution, treating a scenario outcome as a forecast. Furthermore, it is common that scenario users may not realize the full value of scenario planning if they avoid challenging current paradigms—perhaps "we've always done things this way," or "that'll never happen." In practice, scenario planning is a demanding activity. It requires time, effort, and thoughtful consideration by a number of busy people.

6 Summary

Leaders and managers responsible for supply chain risk are faced with issues that are incredibly wide-ranging and complex. In the face of these challenges, traditional risk assessment methods are commonly used to focus attention on the management of specific risks. However, real-world uncertainties present an array of possibilities that far exceed realistic risk management constraints. Rather than overlook uncertain risks, we propose that scenario planning can be used to complement traditional risk assessment methods through the identification and examination of plausible and highly impactful future states. Unlike risk assessment methods that aim to quantify risks by examining probability and impact, the intent of scenario planning is to build awareness of uncertain but plausible risky futures. As decision-makers gain awareness of these risky futures, they are better equipped to recognize signals indicating their emergence, and they can more quickly implement appropriate risk controls.

References

Alcantara, P., Riglietti, G., & Aguada, L. (2017). Report co-sponsored by Business Continuity Institute and Zurich Insurance, PLC. Retrieved from www.the-bci.org.

Bradfield, R., Wright, G., Burt, G., Cairns, G., & Van Der Heijden, K. (2005). The origins and evolution of scenario techniques in long range business planning. *Futures, 37*(8), 795–812.

Chermack, T. J. (2011). *Scenario planning in organizations: How to create, use, and assess scenarios*. San Francisco, CA: Berrett-Koehler.

Chermack, T. J. (2017). *Foundations of scenario planning: The story of Pierre Wack*. New York, NY: Routledge.

Hubbard, D. W. (2009). *The failure of risk management: Why it's broken and how to fix it*. Hoboken, NJ: Wiley.
Kleiner, A. (2008). *The age of heretics: A history of the radical thinkers who reinvented corporate management* (Vol. 164). New Jersey: Wiley.
Milliken, F. J. (1987). Three types of perceived uncertainty about the environment: State, effect, and response uncertainty. *Academy of Management Review, 12*(1), 133–143.
Miranda, V., & Proença, L. M. (1997). Probabilistic choice versus risk analysis-conflicts and synthesis in power system planning (pp. 16–21). IEEE.
Miranda, V., & Proenca, L. M. (1998). Why risk analysis outperforms probabilistic choice as the effective decision support paradigm for power system planning. *IEEE Transactions on Power Systems, 13*(2), 643–648.
Moyer, K. (1996). Scenario planning at British Airways—A case study. *Long Range Planning, 29*(2), 172–181.
Schoemaker, P. J., Day, G. S., & Snyder, S. A. (2013). Integrating organizational networks, weak signals, strategic radars and scenario planning. *Technological Forecasting and Social Change, 80*(4), 815–824.
Schwartz, P. (1996). *The art of the long view: Paths to strategic insight for yourself and your company*. New York, NY: Doubleday.
Wack, P. (1985). Scenarios: Uncharted waters ahead: How royal dutch/shell developed a planning technique that teaches managers to think about an uncertain future. *Harvard Business Review, 63*(5), 73–89.

Chapter 4
Decision Support Systems and Artificial Intelligence in Supply Chain Risk Management

George Baryannis, Samir Dani, Sahar Validi and Grigoris Antoniou

1 Introduction

Over the past two decades, several events have significantly affected global supply chains and have brought the need for management of risks to the forefront. From the 9/11 terrorist attacks and the 2008 economic crisis, to the 2011 Japan earthquake and tsunami (Pettit et al. 2013) and Thailand floods (Chopra and Sodhi 2014), to more recent examples such as the decision in 2016 of the UK to withdraw from the European Union (Matthews 2017) or the KFC chicken supply crisis in early 2018 (Green 2018), global supply chains are disrupted by a multitude of strategic, environmental, financial or political causes. Risks are also becoming more common, as discussed by Snyder et al. (2016) and Behzadi et al. (2017), due to the increased vulnerability of supply chains that adopt lean management and just-in-time production and logistics and the decrease in vertical integration which increases supply chain complexity.

The aforementioned factors have continuously renewed the interest of practitioners and suppliers in research related to risks in supply chains. According to Ho et al. (2015), supply chain risk can be defined as "the likelihood and impact of unexpected macro and/or micro-level events that adversely influence any part of a supply chain,

G. Baryannis (✉) · G. Antoniou
Department of Computer Science, School of Computing & Engineering, University of Huddersfield, Huddersfield, UK
e-mail: g.bargiannis@hud.ac.uk

G. Antoniou
e-mail: g.antoniou@hud.ac.uk

S. Dani · S. Validi
Department of Logistics, Operations, Hospitality and Marketing, Huddersfield Business School, University of Huddersfield, Huddersfield, UK
e-mail: s.s.dani@hud.ac.uk

S. Validi
e-mail: s.validi@hud.ac.uk

G. A. Zsidisin and M. Henke (eds.), *Revisiting Supply Chain Risk*, Springer Series in Supply Chain Management 7, https://doi.org/10.1007/978-3-030-03813-7_4

leading to operational, tactical or strategic level failures or irregularities". Research in supply chain risk is inextricably linked to uncertainty, as the most common cause of risk is the uncertainty of possible outcomes caused by imperfect knowledge or unpredictable events. Addressing risk and uncertainty leads to reduced supply chain vulnerability and reduced impact of disruptions, while achieving higher degrees of robustness and resilience.

Supply chain risk management (SCRM) aims to provide a structured approach to achieve the aforementioned benefits. While there is no universally accepted definition, SCRM generally follows similar risk management strategies in other disciplines in that it consists of at least three phases: identification, assessment and mitigation (Ghadge et al. 2013). These phases depend on the coordination and collaboration of supply chain partners in order to make the correct decisions.

SCRM decision-making reflects the complexity of the supply chain itself, involving the analysis of information from all involved parties and actions that affect anything from individual entities to the whole chain. To that end, operations and supply chain research communities have devoted significant effort in providing decision-makers with the support they need to achieve their SCRM-related goals. This support ranges from methods and techniques that can be used to make more informed decisions, to fully fledged decision support systems. Different techniques are utilised as per the phase in risk management. Some of the techniques employed for risk identification are supply chain vulnerability maps (Blos et al. 2009) and a big data and process engineering approach (Wang et al. 2016). Ghadge et al. (2012) suggest that both qualitative and quantitative methods can be employed for risk assessment. Some of the quantitative techniques involve a supply chain network opportunity package (Brun et al. 2006), a network analysis method to evaluate disruption propagation and its effect on supply chain network (Wu et al. 2007), Petri net (Mazzuto et al. 2012), a data envelopment analysis and Monte Carlo simulation (Wu and Olson 2008), and a fuzzy analytic hierarchy process (Samvedi et al. 2013). Risk mitigation as a process can employ both proactive and reactive strategies. Some of these strategies may include risk-sharing contracts (Ghadge et al. 2017), establishing strategic supplier relationships (Hajmohammad and Vachon 2015), encouraging suppliers' involvement (Chen et al. 2015) and reducing supply base complexity (Olson and Swenseth 2014).

The main purpose of this chapter is to summarise the various techniques that have been used to support decision-making procedures within SCRM and investigate their capabilities, while also determining areas where there is untapped potential that can be leveraged to manage supply chain risks more effectively. Note that the analysis of SCRM research presented in this chapter is representative and by no means exhaustive. Interested readers can indicatively refer to the survey papers of Govindan et al. (2017) and Ho et al. (2015) for a comprehensive literature review of SCRM research.

The rest of this chapter is organised as follows. Section 2 focuses on multiple-criteria decision analysis methods and related techniques that try to find the best out of known solutions to a decision problem. Section 3 deals with methods that rely on mathematical programming to model the decision problem and find optimal solutions. Section 4 focuses on various other artificial intelligence (AI) techniques that have been exploited to support SCRM decision making, namely Petri nets, multi-agent systems, automated reasoning and machine learning. Finally, Sect. 5 concludes and suggests directions to further investigate the synergies between AI and SCRM to facilitate effective decision-making.

2 Multiple-Criteria Decision Analysis for SCRM

The problem of managing risks in supply chains is a prime example of a process relying on multiple-criteria decision analysis (MCDA) and decision making (MCDM), since it entails evaluating the conflicting effects arising both from normal supply chain operation and due to associated risks. Hence, decision support systems for SCRM invariably rely on the vast array of MCDA techniques that have been proposed in the literature. These techniques are usually grouped into two large categories: evaluation techniques, which find the best out of known alternative solutions, and design techniques, which represent the problem as a mathematical problem and solve it to find alternatives (which are initially unknown). In this section, the most prominent techniques belonging to the former category are outlined, along with related techniques that have been used to achieve the same goals, specifically decision trees, game theory and simulation. Section 3 focuses on the latter category, summarising mathematical programming techniques for SCRM.

2.1 MCDA Methods

Analytic Hierarchy Process (AHP): Introduced by Saaty (1980), AHP has become one of the most widely used tools for MCDM under uncertainty. The process involves three main steps: (1) the decision (goal) is decomposed into a hierarchy of alternatives and independent criteria (on one or more levels) that play a role in deciding among the alternatives; (2) a pairwise comparison is conducted between the goal and the criteria, as well as between alternatives and criteria, attributing priorities to all elements; and (3) the calculated priorities are checked for consistency and a decision is made. For instance, 17 different risk factors affecting a supply chain are manually identified in Schoenherr et al. (2008) and included as criteria in AHP in order to decide among five alternative choices for offshore suppliers of a manufacturing company.

Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS): Proposed by Hwang and Yoon (1981), it relies on the notion of geometric distance to evaluate whether an alternative is better or worse. Alternatives and criteria are also pairwise compared like in AHP, and weighted values are attributed to the pairs. Then, two imaginary solutions are constructed: the ideal solution, which has the highest value for all criteria, and the negative ideal, which has the lowest value for all criteria. Finally, the geometric distances from these imaginary solutions are calculated for all alternatives, ranking them according to relative closeness: the optimal alternative is the one that is closest to the ideal and farthest from the negative ideal. Samvedi et al. (2013) combine AHP and TOPSIS in order to create a risk index to determine the severity of risk at a given state of a supply chain. It is noted that the authors employ fuzzy variations of both techniques, where calculated priorities and weights are fuzzy numbers.

Data Envelopment Analysis (DEA): Charnes et al. (1978) introduced this evaluation method for alternative solutions that can be characterised by a set of inputs and a set of outputs. Each solution's efficiency score is the ratio of the weighted sums of outputs and inputs. Weights are calculated using mathematical optimisation, trying to maximise the efficiency of a solution, while making sure that all other efficiencies are reasonable (less than or equal to 1). Azadeh and Alem (2010) propose a decision-making process for supplier selection under uncertainty that relies on fuzzy and stochastic variants of DEA. Input characteristics of suppliers (expected cost, quality acceptance level and on-time delivery distribution rate) and outputs are either modelled as triangular fuzzy numbers, or random variables, depending on whether available data is vague or uncertain.

Failure Mode and Effect Analysis (FMEA): While the aforementioned methodologies are generally applicable to any decision-making process, FMEA is designed to evaluate potential failures of a process and their impact, in order to be able to mitigate failure risk. Hence, it is directly relevant to the goals of SCRM. The FMEA process involves several steps that identify possible failures and their causes, while also evaluating their severity and likelihood of occurring. Then, the current process is evaluated in terms of the likelihood of detecting these failures. Finally, failures are prioritised based on their severity, occurrence and detection likelihood and actions are recommended for each. P.-S. Chen and Wu (2013) approach the supplier selection problem from the perspective of supply chain risk by combining AHP and FMEA. Several criteria for selecting suppliers are identified, and FMEA is used to identify potential cases of suppliers failing to achieve high-quality levels in terms of these criteria, evaluating whether these failures can be detected. Then, AHP is used to calculate weights for each criterion. Finally, failures are prioritised by calculating the product of their severity, occurrence, detection likelihood and AHP weight of the associated criterion.

Table 1 offers a summary and comparison of the aforementioned MCDA evaluation methods, outlining their advantages and disadvantages, the SCRM tasks they are typically used for and some key references.

2.2 *Related Techniques*

Simulation: Many tasks within the SCRM process involve risk-related knowledge that may be unavailable and can be obtained in an exploratory manner. Simulation techniques have proven useful to that end and have been employed either on their own or combined with one of the methods analysed in this and subsequent sections.

Table 1 Comparison of MCDA evaluation methods that have been applied for SCRM

Method	Description	Advantages	Disadvantages	SCRM task	Reference
AHP	Decomposes decision into hierarchy of alternatives based on criteria	Supports both qualitative and quantitative evaluation, group decision making	Problematic to add/remove criteria and alternatives, or when some of these are interdependent	Assess, mitigate	Schoenherr et al. (2008)
TOPSIS	Evaluates alternatives based on difference from ideal solution	Simple and easy to use, fixed number of steps regardless of number of criteria	Euclidean distance calculation does not consider correlation among criteria	Assess, mitigate	Samvedi et al. (2013)
DEA	Maximises efficiency of alternatives by calibrating input/output parameters	Quantifies sources of inefficiency for alternatives	Cannot measure absolute efficiency	Assess, mitigate	Azadeh and Alem (2010)
FMEA	Identifies and evaluates severity and likelihood of failures	Directly applicable to management of risks	Cannot consider combination of failures	Identify, assess	P.-S. Chen and Wu (2013)

For instance, Kull and Closs (2008) use discrete event simulation to assess the supply risk of an organisation and determine which factors contribute more to it. The work of Azadeh and Alem (2010) mentioned earlier uses the Monte Carlo method to simulate the linear models of the proposed DEA variants.

Decision Trees: The inclusion of risks in an analysis of a supply chain leads to the need for representing several different alternative situations, depending on which aspects of the supply chain are affected. Decision trees are a suitable tool for such forms of representation and have been used in SCRM research mostly for risk analysis. For instance, Ruiz-Torres and Mahmoodi (2007) use decision trees to determine the lowest cost approach under various supplier failure scenarios.

Game Theory: Supply chains are a prime example of complex collaboration and competition among players; hence, the related decision-making processes can also be modelled as a game, especially when these decisions involve economy-related risks. For example, Xiao and Yang (2008) apply game theoretic analysis for the case of rival supply chains to determine the effects of suppliers and retailers having different risk profiles (risk-neutral and risk-averse).

3 Mathematical Programming for SCRM

Probably the most utilised methodology to address risks in supply chains involves formalising supply chain interactions as a mathematical optimisation model which seeks to minimise one or more objective functions subject to a number of constraints. In contrast to most of the methodologies presented in Sect. 2, no alternative solutions are known beforehand; they can only be found by solving the models. There is a wide variation in terms of how these models address the inherent uncertainty in risks, as well as how they are solved. The rest of this section attempts to summarise approaches to address both of these aspects, focusing on stochastic programming, robust optimisation and fuzzy programming, in terms of handling uncertainty and exact, heuristic and metaheuristic algorithms in terms of model solving.

3.1 Modelling Uncertainty

Simple mathematical supply chain models include deterministic parameters that are assumed to be fully known. However, this is in contrast to the realities of supply chains where parameters may only partially be known and may be subject to variation, especially due to various risks within or outside the supply chain network. Thus, some degree of uncertainty needs to be integrated into the model parameters. Three different ways have been proposed in the literature to achieve this.

Stochastic Programming: The most common solution is to introduce stochastic parameters for those aspects of the supply chain model that are uncertain, such as demand, supply, return, various aspects of cost and so on. These parameters may be continuous or discrete. In the former case, it is assumed they follow a distribution with known mean and variance, as is the case in the model of Miranda and Garrido (2008) or Taleizadeh et al. (2011), indicatively, where authors model daily demand as a random variable with a fixed mean and variance. Alternatively, uncertain parameters are modelled via a number of discrete scenarios whose occurrence probability is known. The most common case is the so-called two-stage model, where some decisions are made regardless of the values of uncertain parameters (first stage), while the rest follow afterwards and depend on a finite number of realisations of these parameters. In Santoso et al. (2005), for instance, supply chain configuration decisions (e.g. processing centres placement) are fixed, while processing cost, demand, supply and capacity are all considered random variables with a finite number of possible realisations. Finally, a less common approach is to consider more than one period for the second stage or, equivalently, more than two stages. For instance, Nickel et al. (2012) consider multiple periods after the first stage, each with its own possible scenarios, which essentially leads to a tree representation of all scenarios.

Robust Optimisation: If distributions of uncertain parameters are unknown, then the aforementioned solutions are not applicable. Instead, one can assume that parameters vary within a predefined interval or that they follow discrete scenarios for which, however, probabilities are unknown. In such a setting, robust optimisation techniques (Mulvey et al. 1995) can be applied to find an optimal solution across all possible realisations. Specifically, a solution is considered *solution-robust* if it remains close to optimal (e.g. it leads to a minimum increase of the optimal cost), while it is considered *model-robust* if it remains feasible (i.e. does not violate any constraints) for all possible realisations. A notable example is the work of Pishvaee et al. (2011), where the authors consider transportation costs, demand and return to be uncertain in a closed-loop supply chain network and assume that they vary within a prespecified bounded box. The optimisation objective is then to find solutions that satisfy the constraints for all possible realisations of these variables while keeping costs close to the optimal minimum.

Fuzzy Programming: Instead of modelling uncertain parameters as stochastic variables, several works propose to treat them as fuzzy numbers corresponding to a set of possible values with weights attributed according to membership functions, while the corresponding constraints are modelled as fuzzy sets. This leads to so-called fuzzy possibilistic programming solutions that incorporate a level of flexibility in the possible parameter realisations. For instance, Amid et al. (2009) assume that demand follows a triangular function, where the probability of possible demand values ranges from 0 at a lower and an upper limit and peaks at 1 for a value in between. Also, net costs, quality and service levels follow an R-function, where there are two intervals, one corresponding to values of the highest probability, followed by a second one where probability decreases linearly, reaching zero for an upper limit value. On the other hand, Torabi et al. (2015) assume discrete scenarios for demand, supply and cost, with parameter values for each scenario following triangular membership functions.

Table 2 offers a summary and comparison of the aforementioned modelling approaches. It should be noted that there are works which combine the aforementioned techniques into hybrid solutions. For instance, Bai and Liu (2016) models demand and cost as fuzzy numbers but incorporate a robustness element by using variable membership functions instead of fixed ones. Zhalechian et al. (2016) model some aspects of uncertainty using fuzzy numbers, while others are modelled using stochastic chance-constrained programming. Finally, Keyvanshokooh et al. (2016) propose a hybrid robust-stochastic approach, where transportation costs are modelled through stochastic scenarios, while robust optimisation is applied for demand and return quantities which assume to take values from a finite set.

3.2 Model Solving

The mathematical programming techniques analysed above often result in very complex models that are not solvable directly. Stochastic continuous models are most often nonlinear and are usually simplified through linearisation. Scenario-based stochastic models have to be converted to deterministic equivalents, where there is a separate set of constraints for each scenario, resulting in even larger models.

Table 2 Comparison of mathematical programming approaches to modelling uncertainty

Method	Description	Advantages	Disadvantages	Reference
Stochastic programming (SP)	Uses stochastic variable with known distributions to model risk and uncertainty	Granularity can be adapted easily, two-stage model very close to the supply chain decision-making process	Probability distributions must be known for parameters, can become exceptionally complex	Miranda and Garrido (2008), Santoso et al. (2005)
Robust optimisation (RO)	Determines solutions that are nearly optimal or nearly feasible in any realisation	No probability distributions necessary, generally less complex than SP	Delivers more conservative (worst-case) solutions than SP or FP	Pishvaee et al. (2011)
Fuzzy programming (FP)	Uses fuzzy numbers to model risk and uncertainty	Models ambiguity and vagueness, generally more tractable than SP	Models are more difficult to grasp, requires more expertise	Amid et al. (2009), Torabi et al. (2015)

Fuzzy models are also reformulated to their crisp (defuzzified) equivalents, interpreting membership degrees of fuzzy sets using real values. Then, depending again on the complexity of the resulting model, one of the solution approaches described in the rest of this section is followed.

Commercial Solvers: In many cases, the resulting model is solvable using a proprietary optimisation software package in a reasonable amount of time. Modelling and optimisation systems commonly referenced in the literature include CPLEX,[1] GAMS,[2] LINGO[3] and GUROBI.[4]

Optimal Solution Algorithms: In other cases, well-known algorithms are employed, which have been proven capable of finding the optimal solution, provided that the model possesses specific characteristics. For instance, Santoso et al. (2005) apply Benders (or L-shaped) decomposition (Benders 1962) to solve the proposed model, relying on the fact that a two-stage stochastic program can be easily divided into sub-problems. A similar divide-and-conquer approach is followed in the Branch and Bound algorithm (Land and Doig 1960), which is employed by Qi et al. (2010) in their attempt to investigate the effects of supply and demand disruptions on retailer location and customer allocation.

Heuristic Algorithms: Model complexity may preclude finding an optimal solution, either because it requires unacceptable amounts of time or because the aforementioned algorithms fail to find such an exact solution. In such cases, heuristic algorithms are employed to find a good enough or an approximate solution. Proba-

[1] https://www.ibm.com/analytics/data-science/prescriptive-analytics/cplex-optimizer.

[2] http://www.gams.com.

[3] https://www.lindo.com/index.php/products/lingo-and-optimization-modeling.

[4] http://www.gurobi.com/products/gurobi-optimizer.

bly the most common heuristic used in supply chain research is Lagrangian relaxation (LR) (Everett 1963) which uses multipliers to penalise violations of constraints and tries to minimise these values.

Metaheuristic Algorithms: In other cases, standard heuristics are not able to find sufficiently good solutions, so a metaheuristic algorithm is employed to find or generate better heuristics. Many metaheuristics are inspired by nature, such as genetic algorithms (GA) which simulate the process of natural selection. Simulated annealing (SA) parallels the process of heating and slowly cooling materials in metallurgy with that of slowly decreasing the probability of accepting worse solutions while trying to find an optimal one. Peng et al. (2011) use a GA-based metaheuristic for a model that attempts to reduce the risk of facility disruptions, while Lee and Dong (2009) address the typical problem of uncertain demand and return for reverse logistic networks using an SA-based algorithm to decide on facility locations and product flow. Other metaheuristics rely on local search methods, trying to improve on a candidate solution by slightly changing it. Cardona-Valdés et al. (2014) combine two such metaheuristics, GRASP and Tabu search, to address demand uncertainty in the decision-making process for warehouse location and transportation mode allocation.

4 AI Techniques for SCRM

The methods discussed in Sect. 2 focus primarily on integrating the opinions of stakeholders and partially automating the process of weighing the various criteria that factor in a decision. The mathematical programming techniques in Sect. 3 can broadly be considered as part of the AI field, since they apply intelligent methods of searching for a solution and are able to do so faster due to the constantly increasing computational capabilities of machines. However, the intelligence of such techniques is still constrained. This section explores other AI techniques that have received relatively little attention in supply chain research and discuss how these may prove useful to decision making for SCRM.

4.1 Petri Nets

Viewed from a high level of abstraction, supply chains can be considered as discrete event dynamic systems, since their evolution is directly dependent on the occurrence of events over time. This is especially true when these events have significant effects on their operation, as is the case of risk events. The analysis of such systems usually relies on some kind of graph model, like Petri nets (Petri 1966). Petri nets consist of three types of elements: (1) places, modelling states; (2) transitions, modelling the transition from one place to another; and (3) arcs, connecting an initiating place to a transition and a transition to a subsequent place. Each place may have one or more tokens. For a transition to fire (i.e. occur), a predefined sufficient number of tokens must be present at the place leading to that transition.

Petri net models essentially represent cause and effect relationships which are fundamental in risk analysis. This has been recognised in SCRM literature by a handful of researchers. Asar et al. (2006) use fault tree analysis to identify multiple levels of causes of disruption in a manufacturing supply chain, as well as existing mitigating techniques. The resulting fault tree is then converted to a Petri net, which is then used to determine the probability levels for each disruption and the success level of mitigation practices. Rossi and Pero (2012) follow a different approach, modelling the complete operation of a simple logistic network as a Petri net. Any product-related element is represented by a token (e.g. customer requests, occurred stock-outs, order quantities, safety stocks). Risks are then identified by calculating the coverability graph of the Petri net, e.g. detecting cases where delivery lead times are higher than a threshold, or cases of inaccurate forecasts at the retailer or distributor side.

Zegordi and Davarzani (2012) use a well-known variant called coloured Petri nets which provide the ability to distinguish between tokens, using values called colours. These are employed to model the interconnected relationships among disruptions: each type of disruption is assigned a colour and when one disruption may cause another, a token is allowed to change colour. The graphs represent the supply chain operation as in Rossi and Pero (2012) and their analysis helps determine how disruptions propagate and how they affect performance.

4.2 Multi-agent Systems

A supply chain involves a number of entities (customers, suppliers and so on) interacting with each other, each with their own agendas, which may sometimes overlap or conflict. It is straightforward to imagine each one of these entities as an intelligent agent, model the supply chain as a multi-agent system (MAS) and use this system to support decision making. In such an MAS, each agent follows a set of rules that govern its interactions with the other agents. Agents communicate with each other by issuing requests and responses. In principle, after defining each agent's behaviour, an MAS can run independently and reach a solution without the need for human intervention, since agents are capable of perceiving their environment, respond to changes and initiate actions.

Kwon et al. (2007) propose the use of MAS to address supply and demand uncertainties in manufacturing supply chain management. Three types of agents are modelled: retailers, manufacturers and suppliers. Each agent makes decisions according to the interests of the firm it represents and can adjust its behaviour to respond to risks. For instance, a manufacturer agent aims to maximise revenue and minimise costs, while it has to decide on order and production quantities and whether to expand its supplier base to address supply risk. The authors propose an iterative adjustment approach so that all agents achieve their profit goals, while the supply chain's profit is also maximised. Simulations are run with varying numbers for customer demand, lead time, production capacity and number of suppliers, while the manufacturer includes a risk pooling strategy in its behaviour to search for additional suppliers in the face of disruptions.

Mele et al. (2007) combine an MAS with Monte Carlo simulation and metaheuristics to retrofit a supply chain design due to uncertain demand, as well as transport and processing times. Specifically, a genetic algorithm is used to determine inventory control parameters. Then, different realisations of the uncertain parameters are obtained using Monte Carlo sampling. All parameter values are fed into the MAS which aims to maximise profit by emulating the decision-making process in terms of production scheduling, transport of materials and inventory replenishment. This process is iterated (applying genetic operators and generating new samples) until optimality criteria are met.

Giannakis and Louis (2011) present a holistic MAS framework for all phases of SCRM. Apart from agents representing supply chain entities, there are additional ones to support communication, coordination, monitoring and disruption management. Risk identification relies on the monitoring agent detecting changes in performance indicators such as in-stock inventory, production throughput or delivery lead times. Assessment is then run by the disruption management agent, who investigates the root cause for each risk and determines risk impacts and probabilities. Then, past responses to each risk are collected in risk portfolios and evaluated, simulating their effects using the MAS. Finally, the best performing risk responses are proposed as solutions.

4.3 Automated Rule-Based Reasoning

Decision making for SCRM and supply chain management in general has always relied on the accumulated expertise and experience of key stakeholders. Automated reasoning systems provide a means of encoding this knowledge into a machine-interpretable form in order to (partially) automate the decision-making process. A common approach is to rely on a rule-based representation (with case-based being a popular alternative). Rules have the advantage of being easily interpretable by both humans and machines, since they follow a simple if-then formalisation.

SCRIS (Kayis and Karningsih 2012) is a supply chain risk identification system that relies on rule-based knowledge encoded using the CLIPS[5] language. The authors elicit knowledge from existing SCRM literature to collect supply chain risk events, factors and sub-factors and their interrelations. These are expressed in the form of a rule hierarchy that facilitates a forward chaining inference approach: specific characteristics of a supply chain lead to the identification of risk sub-factors, sub-factors lead to factors, factors to events, and finally events to communication of

[5] http://www.clipsrules.net.

identified risks. SCRIS is validated using several case studies, showing that it can identify 80% of potential risks.

Emmenegger et al. (2012) propose an early warning system for procurement risks in supply chains that relies on information sources both internal to the supply chain and external (e.g. business information services or the Internet), which indicate the existence of a risk event. The system relies on an ontological risk model that includes enterprise semantics, risk events, risk indicators, warning signals and procurement risks. The ontology is written in OWL[6] and rules are encoded in SQWRL (O'Connor and Das 2009), while the identification process is as follows: risk events that are derived from information sources are aggregated and contribute to the calculation of risk indicators. If these exceed a threshold, then a warning signal is issued. A particular risk is identified when all warning signals associated with it are issued.

4.4 Machine Learning

The past decade has seen a tremendous growth in research on and applications of machine learning, a research area within AI focusing on systems that are not only intelligent in the sense of deriving conclusions and making decisions but also due to their ability to learn in order to improve their performance. While machine learning principles have existed since the birth of AI as a research field (and even earlier, in the case of statistical methods), research has progressed rapidly in recent years, partly due to the increase in available computing power and the emergence of big data. While advances in machine learning have been exploited in various research areas, their application in SCRM has only been considered by a few studies, which are analysed in the rest of this section.

The first study, to our knowledge, to incorporate machine learning in SCRM-related tasks is that of Bruzzone and Orsoni (2003). The authors use Artificial Neural Networks (ANNs), one of the earliest successes in machine learning research, to assess logistic performance risks in terms of actual transportation costs and production losses. ANNs are fed input data on production times, quantities and capacities. Then, they are trained using calculated cost estimates for the available input. This gives them the ability to learn to calculate cost estimates for different sets of input data. Evaluation results prove the superiority of ANNs in terms of flexibility, adaptability and accuracy of response, compared to discrete event simulation.

ANNs are combined with a case-based reasoning (CBR) system in Zhao and Yu (2011) to address the problem of supplier selection under uncertainty for the case of Chinese petroleum enterprises. CBR relies on the principle that if a solution was successful in the past, it may also be successful in closely similar situations. The authors propose to use ANNs to improve on key problems of CBR: (1) how to objectively calculate suitable weights for all attributes that characterise a case; (2) how to determine the degree of similarity between existing cases and the target

[6] https://www.w3.org/TR/owl2-overview.

case; (3) how to extract rules from the cases; and (4) how to maintain the case base. ANNs are trained using existing cases and then use this knowledge to learn how to determine decisions for new cases, which are in turn expressed as new cases and stored in the case base to be used for future decisions.

The CBR approach is also adopted by Jiang and Sheng (2009) for the problem of inventory control under demand risk. Previous cases of replenishment actions using order-up-to levels or reorder points are collected, along with the achieved service levels. Then, a reinforcement learning approach is applied to make decisions for new cases, in terms of order-up-to levels or reorder points. The achieved service level is the actual reward (or punishment, if it is unsatisfactory) that helps the system learn which actions bring it closer to or further from the target service level. Results show that reinforcement learning achieves average service levels that are very close to the target level, especially in the case of reorder point replenishment.

Chen et al. (2010) propose the use of a Bayesian model for the management of manufacturing supply chains that face supply disruptions. This relies on Bayes' rule which relates the conditional probability of an event A happening given evidence B, to the probability of A happening (in general), the probability of B being observed, and the probability of B being observed given that A happened. This allows recalculating probabilities after new evidence is acquired. The authors' model assumes that disruptions affect supply in a number of fixed levels, each with an unknown probability. The goal of the model is to learn these probabilities over time, starting with initial values determined from past experience, expert assessment or provided by suppliers themselves. By learning these probabilities, the manufacturer can make informed decisions about sourcing strategies, even when the initial knowledge is imperfect.

Bayes' rule is also featured in Garvey et al. (2015) in the form of Bayesian (Belief) Networks (BN). These graph models represent events that have a direct influence on others. Based on these connections, one can calculate the probability of an event taking place, given that others have also taken place. The authors model a set of risks as a BN and use it within the risk assessment process to determine how risk propagates. Each member of a supply network (distributors, manufacturers, retailers) is then evaluated in terms of their risk contribution factor and risk propagation ratio.

The work of Zage et al. (2013) is unique since it is the only published SCRM study, to the best of our knowledge, that combines a machine learning approach with an implementation that exploits big data. The authors focus on security risks in supply chains, specifically the problem of identifying deceptive practices in e-commerce. First, they use a graph-based representation of transactions to determine relationships that are characteristics of deception. Then, they use these characteristics as features in a clustering approach to distinguish legitimate users (those who do not exhibit such characteristics) and fraudsters. The algorithm relies on large-scale Web data, collecting information for vendors through their Web presence. Evaluation shows that high accuracy in detecting fraudsters is achieved even when the classifier is trained with only one-third of the available data. Table 3 provides a summary and comparison of all AI techniques presented in this section.

Table 3 Comparison of AI techniques that have been applied for SCRM

Technique	Description	Advantages	Disadvantages	SCRM task	Reference
Petri nets	Model dynamic systems in the form of states and transitions between them	Can be used at various levels of abstraction, supports automatic simulation	May be difficult to build, maintain and interpret if network is too large	Identify, assess	Asar et al. (2006), Zegordi and Davarzani (2012)
Multi-agent systems	Simulate interactions between entities with predefined behaviour	Can rapidly react and adapt to changing environments, scales easily	Formalising agent behaviour requires expertise and may become too complex	Identify, assess, mitigate	Mele et al. (2007), Giannakis and Louis (2011)
Automated rule-based reasoning	Encode knowledge using rules, infer information and choose actions	Natural, intuitive way to encode expert knowledge, modular, powerful reasoning systems	Rules need to be carefully crafted to avoid loops or contradictions, may require large rule sets	Identify, assess, mitigate	Kayis and Karningsih (2012), Emmenegger et al. (2012)
Machine learning	Learn from existing knowledge and make predictions on previously unknown set-ups	Uncovers hidden correlation in data, continuously improves as more data becomes available	Depends on the availability of relevant and accurate datasets, results may not be interpretable	Identify, assess, mitigate	P.-S. Chen and Wu (2013)

5 Conclusions

The wide variety of available methods and techniques presented in this chapter supports the fact that supply chain decision-makers have access to a powerful arsenal in their quest to manage risks that affect the supply chain. This gives them the ability to choose the tools that are most suitable to their goals. From our analysis, we can draw the following conclusions:

- MCDA analysis methods such as AHP, TOPSIS, DEA or FMEA are more suitable when the various alternative choices are known and the decision-maker needs a structured and systematic way of deciding among them. This makes them especially suitable for deciding among different risk mitigation plans.

- Mathematical modelling and optimisation excel at capturing the full spectrum of parameters, constraints and objectives that are involved in a supply chain decision and can provide optimal or close to optimal solutions for highly complex models. Thus, they are suited for the case when a supply chain can be modelled in detail, the target objectives are fully known, but the different ways of achieving these objectives are not completely known. In such cases, mathematical optimisation can derive risk mitigation decisions and plans that achieve SCRM-related objectives.
- AI techniques are very diverse, which means that their success depends on choosing the suitable technique for the task at hand. For instance, network-based approaches like Petri nets are especially suitable when one needs to trace interactions and assess the dynamic behaviour of a supply chain. Multi-agent systems can place more focus on the conflicting or coordinating interactions among different supply chain stakeholders. Rule-based reasoning techniques are excellent when knowledge can be easily encoded in the form of rules. Finally, machine learning techniques can support a wide variety of tasks but can only do so effectively when an adequate amount of data is available.

Since each technique has its own set of capabilities and may be more suitable for some aspects of SCRM than others (as summarised in Tables 1, 2 and 3), it makes sense to explore the possibility of combining two or more of the presented methods and techniques into a comprehensive decision support system for SCRM. While some cases of hybridisation have been reported in the literature [e.g. in the work of Keyvanshokooh et al. (2016)], they usually follow specific patterns, such as the introduction of fuzziness into existing techniques, or the combination of mathematical programming with MCDA analysis methods. However, it would also be interesting to explore a hybrid approach that integrates one of the AI techniques in Sect. 4 with the powerful optimisation abilities of mathematical programming.

Finally, what should be evident from the discussion in Sect. 4 is that while research in AI techniques has made great strides in recent years, SCRM and operations research, in general, have not fully exploited the associated benefits. In particular, the powerful predictive and learning capabilities of machine learning and big data analytics have an indisputable potential that can revolutionise SCRM, both with regard to identifying and assessing risks more quickly and accurately and determining the optimal ways to respond to them in order to create more robust and resilient supply chains.

References

Amid, A., Ghodsypour, S. H., & O'Brien, C. (2009). A weighted additive fuzzy multiobjective model for the supplier selection problem under price breaks in a supply chain. *International Journal of Production Economics, 121*(2), 323–332. https://doi.org/10.1016/j.ijpe.2007.02.040.

Asar, A., Meng, C. Z., Caudill, R. J., & Asar, S. (2006). Modelling risks in supply chains using Petri net approach. *International Journal of Services Operations and Informatics, 1*(3), 273–285. https://doi.org/10.1504/ijsoi.2006.011016.

Auswirkungen des Brexits auf die Agrar- und Lebensmittelexporte Irlands in das Vereinigte Königreich. *EuroChoices, 16*(2), 26–32. https://doi.org/10.1111/1746-692x.12160.
Azadeh, A., & Alem, S. M. (2010). A flexible deterministic, stochastic and fuzzy data envelopment analysis approach for supply chain risk and vendor selection problem: Simulation analysis. *Expert Systems with Applications, 37*(12), 7438–7448. https://doi.org/10.1016/j.eswa.2010.04.022.
Bai, X., & Liu, Y. (2016). Robust optimization of supply chain network design in fuzzy decision system. *Journal of Intelligent Manufacturing, 27*(6), 1131–1149. https://doi.org/10.1007/s10845-014-0939-y.
Behzadi, G., O'Sullivan, M. J., Olsen, T. L., & Zhang, A. (2017). Agribusiness supply chain risk management: A review of quantitative decision models. *Omega (United Kingdom)*. https://doi.org/10.1016/j.omega.2017.07.005.
Benders, J. F. (1962). Partitioning procedures for solving mixed-variables programming problems. *Numerische Mathematik, 4*(1), 238–252. https://doi.org/10.1007/bf01386316.
Blos, M. F., Quaddus, M., Wee, H. M., & Watanabe, K. (2009). Supply chain risk management (SCRM): A case study on the automotive and electronic industries in Brazil. *Supply Chain Management: An International Journal, 14*(4), 247–252. https://doi.org/10.1108/13598540910970072.
Brun, A., Caridi, M., Fahmy Salama, K., & Ravelli, I. (2006). Value and risk assessment of supply chain management improvement projects. *International Journal of Production Economics, 99*(1), 186–201. https://doi.org/10.1016/j.ijpe.2004.12.016.
Bruzzone, A., & Orsoni, A. (2003). AI and simulation-based techniques for the assessment of supply chain logistic performance. *2003-January*, 154–164. https://doi.org/10.1109/simsym.2003.1192809.
Cardona-Valdés, Y., Álvarez, A., & Pacheco, J. (2014). Metaheuristic procedure for a bi-objective supply chain design problem with uncertainty. *Transportation Research Part B: Methodological, 60,* 66–84. https://doi.org/10.1016/j.trb.2013.11.010.
Charnes, A., Cooper, W. W., & Rhodes, E. (1978). Measuring the efficiency of decision making units. *European Journal of Operational Research, 2*(6), 429–444. https://doi.org/10.1016/0377-2217(78)90138-8.
Chen, J., Zhao, X., & Shen, Z.-J. (2015). Risk mitigation benefit from backup suppliers in the presence of the horizontal fairness concern. *Decision Sciences, 46*(4), 663–696. https://doi.org/10.1111/deci.12157.
Chen, M., Xia, Y., & Wang, X. (2010). Managing supply uncertainties through Bayesian information update. *IEEE Transactions on Automation Science and Engineering, 7*(1), 24–36. https://doi.org/10.1109/tase.2009.2018466.
Chen, P.-S., & Wu, M.-T. (2013). A modified failure mode and effects analysis method for supplier selection problems in the supply chain risk environment: A case study. *Computers & Industrial Engineering, 66*(4), 634–642. https://doi.org/10.1016/j.cie.2013.09.018.
Chopra, S., & Sodhi, M. S. (2014). Reducing the risk of supply chain disruptions. *MIT Sloan Management Review, 55,* 73–80.
Emmenegger, S., Laurenzi, E., & Thönssen, B. (2012). Improving supply-chain-management based on semantically enriched risk descriptions. In K. Liu & J. Filipe (Eds.), *Proceedings of the International Conference on Knowledge, Management and Information Sharing* (pp. 70–80).
Everett, H. (1963). Generalized lagrange multiplier method for solving problems of optimum allocation of resources. *Operations Research, 11*(3), 399–417. https://doi.org/10.1287/opre.11.3.399.
Garvey, M. D., Carnovale, S., & Yeniyurt, S. (2015). An analytical framework for supply network risk propagation: A Bayesian network approach. *European Journal of Operational Research, 243*(2), 618–627. https://doi.org/10.1016/j.ejor.2014.10.034.
Ghadge, A., Dani, S., & Kalawsky, R. (2012). Supply chain risk management: Present and future scope. *The International Journal of Logistics Management, 23*(3), 313–339. https://doi.org/10.1108/09574091211289200.

Ghadge, A., Dani, S., Chester, M., & Kalawsky, R. (2013). A systems approach for modelling supply chain risks. *Supply Chain Management: An International Journal, 18*(5), 523–538. https://doi.org/10.1108/SCM-11-2012-0366.

Ghadge, A., Dani, S., Ojha, R., & Caldwell, N. (2017). Using risk sharing contracts for supply chain risk mitigation: A buyer-supplier power and dependence perspective. *Computers & Industrial Engineering, 103,* 262–270. https://doi.org/10.1016/j.cie.2016.11.034.

Giannakis, M., & Louis, M. (2011). A multi-agent based framework for supply chain risk management. *Journal of Purchasing and Supply Management, 17*(1), 23–31. https://doi.org/10.1016/j.pursup.2010.05.001.

Govindan, K., Fattahi, M., & Keyvanshokooh, E. (2017). Supply chain network design under uncertainty: A comprehensive review and future research directions. *European Journal of Operational Research, 263*(1), 108–141. https://doi.org/10.1016/j.ejor.2017.04.009.

Green, W. (2018). Five lessons from the KFC chicken crisis. *CIPS Supply Management*. https://www.cips.org/supply-management/analysis/2018/february/five-lessons-from-the-kfc-chicken-crisis/.

Hajmohammad, S., & Vachon, S. (2015). Mitigation, avoidance, or acceptance? Managing supplier sustainability risk. *Journal of Supply Chain Management, 52*(2), 48–65. https://doi.org/10.1111/jscm.12099.

Ho, W., Zheng, T., Yildiz, H., & Talluri, S. (2015). Supply chain risk management: A literature review. *International Journal of Production Research, 53*(16), 5031–5069. https://doi.org/10.1080/00207543.2015.1030467.

Hwang, C.-L., & Yoon, K. (1981). *Multiple attribute decision making (Lecture notes in economics and mathematical systems)*. Berlin: Springer.

Jiang, C., & Sheng, Z. (2009). Case-based reinforcement learning for dynamic inventory control in a multi-agent supply-chain system. *Expert Systems with Applications, 36*(3 Part 2), 6520–6526. https://doi.org/10.1016/j.eswa.2008.07.036.

Kayis, B., & Karningsih, P. D. (2012). SCRIS: A knowledge-based system tool for assisting manufacturing organizations in identifying supply chain risks. *Journal of Manufacturing Technology Management, 23*(7), 834–852. https://doi.org/10.1108/17410381211267682.

Keyvanshokooh, E., Ryan, S. M., & Kabir, E. (2016). Hybrid robust and stochastic optimization for closed-loop supply chain network design using accelerated Benders decomposition. *European Journal of Operational Research, 249*(1), 76–92. https://doi.org/10.1016/j.ejor.2015.08.028.

Kull, T., & Closs, D. (2008). The risk of second-tier supplier failures in serial supply chains: Implications for order policies and distributor autonomy. *European Journal of Operational Research, 186*(3), 1158–1174. https://doi.org/10.1016/j.ejor.2007.02.028.

Kwon, O., Im, G. P., & Lee, K. C. (2007). MACE-SCM: A multi-agent and case-based reasoning collaboration mechanism for supply chain management under supply and demand uncertainties. *Expert Systems with Applications, 33*(3), 690–705. https://doi.org/10.1016/j.eswa.2006.06.015.

Land, A. H., & Doig, A. G. (1960). An automatic method of solving discrete programming problems. *Econometrica, 28*(3), 497–520. https://doi.org/10.2307/1910129.

Lee, D. H., & Dong, M. (2009). Dynamic network design for reverse logistics operations under uncertainty. *Transportation Research Part E: Logistics and Transportation Review, 45*(1), 61–71. https://doi.org/10.1016/j.tre.2008.08.002.

Les incidences du Brexit sur les exportations irlandaises de produits agroalimentaires vers le Royaume-Uni.

Matthews, A. (2017). Brexit impacts on Irish agri-food exports to the UK. *EuroChoices, 16,* 26–32.

Mazzuto, G., Bevilacqua, M., & Ciarapica, F. E. (2012). Supply chain modelling and managing, using timed coloured Petri nets: A case study. *International Journal of Production Research, 50*(16), 4718–4733. https://doi.org/10.1080/00207543.2011.639397.

Mele, F. D., Guillén, G., Espuña, A., & Puigjaner, L. (2007). An agent-based approach for supply chain retrofitting under uncertainty. *Computers & Chemical Engineering, 31*(5–6), 722–735. https://doi.org/10.1016/j.compchemeng.2006.12.013.

Miranda, P. A., & Garrido, R. A. (2008). Valid inequalities for Lagrangian relaxation in an inventory location problem with stochastic capacity. *Transportation Research Part E: Logistics and Transportation Review, 44*(1), 47–65. https://doi.org/10.1016/j.tre.2006.04.002.

Mulvey, J. M., Vanderbei, R. J., & Zenios, S. A. (1995). Robust optimization of large-scale systems. *Operations Research, 43*(2), 264–281. https://doi.org/10.1287/opre.43.2.264.

Nickel, S., Saldanha-da-Gama, F., & Ziegler, H. P. (2012). A multi-stage stochastic supply network design problem with financial decisions and risk management. *Omega, 40*(5), 511–524. https://doi.org/10.1016/j.omega.2011.09.006.

O'Connor, M., & Das, A. (2009). *SQWRL: a query language for OWL.* Paper presented at the Proceedings of the 6th International Conference on OWL: Experiences and Directions—Volume 529, Chantilly, VA,.

Olson, D. L., & Swenseth, S. R. (2014). Trade-offs in supply chain system risk mitigation. *Systems Research and Behavioral Science, 31*(4), 565–579. https://doi.org/10.1002/sres.2299.

Peng, P., Snyder, L. V., Lim, A., & Liu, Z. (2011). Reliable logistics networks design with facility disruptions. *Transportation Research Part B: Methodological, 45*(8), 1190–1211. https://doi.org/10.1016/j.trb.2011.05.022.

Petri, C. A. (1966). *Communication with automata*. Hamburg.

Pettit, T. J., Croxton, K. L., & Fiksel, J. (2013). Ensuring supply chain resilience: Development and implementation of an assessment tool. *Journal of Business Logistics, 34*(1), 46–76. https://doi.org/10.1111/jbl.12009.

Pishvaee, M. S., Rabbani, M., & Torabi, S. A. (2011). A robust optimization approach to closed-loop supply chain network design under uncertainty. *Applied Mathematical Modelling, 35*(2), 637–649. https://doi.org/10.1016/j.apm.2010.07.013.

Qi, L., Shen, Z. J. M., & Snyder, L. V. (2010). The effect of supply disruptions on supply chain design decisions. *Transportation Science, 44*(2), 274–289. https://doi.org/10.1287/trsc.1100.0320.

Rossi, T., & Pero, M. (2012). A formal method for analysing and assessing operational risk in supply chains. *International Journal of Operational Research, 13*(1), 90–109. https://doi.org/10.1504/ijor.2012.044029.

Ruiz-Torres, A. J., & Mahmoodi, F. (2007). The optimal number of suppliers considering the costs of individual supplier failures. *Omega, 35*(1), 104–115. https://doi.org/10.1016/j.omega.2005.04.005.

Saaty, T. L. (1980). *The analytic hierarchy process: Planning, priority setting, resources allocation* (p. 281). New York: McGraw.

Samvedi, A., Jain, V., & Chan, F. T. S. (2013). Quantifying risks in a supply chain through integration of fuzzy AHP and fuzzy TOPSIS. *International Journal of Production Research, 51*(8), 2433–2442. https://doi.org/10.1080/00207543.2012.741330.

Santoso, T., Ahmed, S., Goetschalckx, M., & Shapiro, A. (2005). A stochastic programming approach for supply chain network design under uncertainty. *European Journal of Operational Research, 167*(1), 96–115. https://doi.org/10.1016/j.ejor.2004.01.046.

Schoenherr, T., Tummala, V. M. R., & Harrison, T. P. (2008). Assessing supply chain risks with the analytic hierarchy process: Providing decision support for the offshoring decision by a US manufacturing company. *Journal of Purchasing and Supply Management, 14*(2), 100–111. https://doi.org/10.1016/j.pursup.2008.01.008.

Snyder, L. V., Atan, Z., Peng, P., Rong, Y., Schmitt, A. J., & Sinsoysal, B. (2016). OR/MS models for supply chain disruptions: A review. *IIE Transactions (Institute of Industrial Engineers), 48*(2), 89–109. https://doi.org/10.1080/0740817x.2015.1067735.

Taleizadeh, A. A., Niaki, S. T. A., & Barzinpour, F. (2011). Multiple-buyer multiple-vendor multi-product multi-constraint supply chain problem with stochastic demand and variable lead-time: A harmony search algorithm. *Applied Mathematics and Computation, 217*(22), 9234–9253. https://doi.org/10.1016/j.amc.2011.04.001.

Torabi, S. A., Baghersad, M., & Mansouri, S. A. (2015). Resilient supplier selection and order allocation under operational and disruption risks. *Transportation Research Part E: Logistics and Transportation Review, 79,* 22–48. https://doi.org/10.1016/j.tre.2015.03.005.

Wang, G., Gunasekaran, A., Ngai, E. W. T., & Papadopoulos, T. (2016). Big data analytics in logistics and supply chain management: Certain investigations for research and applications. *International Journal of Production Economics, 176,* 98–110. https://doi.org/10.1016/j.ijpe.2016.03.014.

Wu, T., Blackhurst, J., & O'Grady, P. (2007). Methodology for supply chain disruption analysis. *International Journal of Production Research, 45*(7), 1665–1682. https://doi.org/10.1080/00207540500362138.

Wu, D. D., & Olson, D. L. (2008). Supply chain risk, simulation, and vendor selection. *International Journal of Production Economics, 114*(2), 646–655. https://doi.org/10.1016/j.ijpe.2008.02.013.

Xiao, T., & Yang, D. (2008). Price and service competition of supply chains with risk-averse retailers under demand uncertainty. *International Journal of Production Economics, 114*(1), 187–200. https://doi.org/10.1016/j.ijpe.2008.01.006.

Zage, D., Glass, K., & Colbaugh, R. (2013). Improving supply chain security using big data. 254–259. https://doi.org/10.1109/isi.2013.6578830.

Zegordi, S. H., & Davarzani, H. (2012). Developing a supply chain disruption analysis model: Application of colored Petri-nets. *Expert Systems with Applications, 39*(2), 2102–2111. https://doi.org/10.1016/j.eswa.2011.07.137.

Zhalechian, M., Tavakkoli-Moghaddam, R., Zahiri, B., & Mohammadi, M. (2016). Sustainable design of a closed-loop location-routing-inventory supply chain network under mixed uncertainty. *Transportation Research Part E: Logistics and Transportation Review, 89,* 182–214. https://doi.org/10.1016/j.tre.2016.02.011.

Zhao, K., & Yu, X. (2011). A case based reasoning approach on supplier selection in petroleum enterprises. *Expert Systems with Applications, 38*(6), 6839–6847. https://doi.org/10.1016/j.eswa.2010.12.055.

Chapter 5
Resilience Assessment in Complex Supply Networks

Mustafa Güller and Michael Henke

1 Introduction

In today's business environment, the local marketing strategy is shifting away to modern value chains which span the entire globe. However, the opportunities created by the globalization of supply chains bring new challenges. With globalization, supply chains have become more vulnerable to disruptions (Tang and Tomlin 2008). As the network extends over the entire globe, the number of links interconnecting companies is growing significantly. These links are often prone to disruptions, bankruptcies, breakdowns, and disasters, increasing the possibility for unplanned events (Manuj and Mentzer 2008). Furthermore, the structure of supply chains is shifting away from the "chain structure" toward "a network of interacting entities." Hence, a supply network can be considered as a network of (semi)autonomous organizations that make decisions independently. These organizations usually work in a distributed and decentralized manner in such a complex network (Chan and Chan 2010; Hongler et al. 2010). The increasing length of networks, in conjunction with nonlinear and dynamic interactions between nodes, adds a new level of complexity to the decision-making process. Even though they follow simple local rules, they generate complex patterns of decisions due to relationships among them (Nair et al. 2009). One major problem in such networks is to manage and mitigate risks across multiple independent organizations.

Risks can cause negligible problems like a short delay of a transport or, at the other end of the spectrum, a total breakdown of the entire supply chain (SC) net-

M. Güller (✉)
TU Dortmund University, Dortmund, Germany
e-mail: guller@lfo.tu-dortmund.de

M. Henke
TU Dortmund University, Fraunhofer Institute for Material Flow and Logistics IML, Dortmund, Germany
e-mail: michael.henke@iml.fraunhofer.de

G. A. Zsidisin and M. Henke (eds.), *Revisiting Supply Chain Risk*, Springer Series in Supply Chain Management 7, https://doi.org/10.1007/978-3-030-03813-7_5

work due to a natural disaster. More recently, two natural disasters in Asia, the 2011 Tohoku earthquake in Japan and the severe flooding during the monsoon season in Thailand, caused serious disruptions in a number of industries (e.g., the automotive and electronics industries). Such risks may occur at any node in the network and affect other business partners due to interdependencies in flows of goods, financial flows, and flows of information. This motivates firms to rethink their understanding of the structure and interlinkages of their supply networks. Another example is the flood caused by Hurricane Floyd in North Carolina which flooded a Daimler Chrysler plant located in Greenville that is responsible for manufacturing automotive components. As a result, seven assembly plants across North America had to be shut down for seven days (Jüttner 2005). From the aforementioned examples, it can be realized that suppliers are inevitable sources of external risks in any supply network (Rajesh and Ravi 2015), particularly for firms that operate internationally. The results of a recent survey (Snell 2010) illustrated that 90% of firms felt threatened by supply-side risks. However, 60% of the firms noted that they were not confident or knowledgeable enough in managing these risks. Most firms face the risk of disruption to their supply due to accidents at supplier facilities, bankruptcy of a key supplier, labor strikes, defective parts or components, natural disasters, terrorism, or other events. Despite the diversity of causes, supply risks generally fall into three categories: the disruption of supply caused by low likelihood events such as natural disasters or terroristic activities, random yield due to capacity and quality issues, and price volatility resulting from fluctuating exchange rates (Tomlin and Synder 2008).

Resilience has been widely used as one of the core elements to deal with and to respond to such major disruptions. Therefore, building resilient supply networks has become an important issue for managers, stakeholders, and researchers (Kleindorfer and Saad 2005; Ponoramov and Holcomb 2009). Despite a large body of the literature on resilience, there is no generally accepted or generalized standard for measuring resilience of complex systems (Kamalahmadi and Parast 2016; Spiegler et al. 2012). Spiegler et al. conclude from a literature review that most existing studies have proposed qualitative methods in which resilience metrics depend on personal judgment by managers. These qualitative methods are not suitable for investigating 'what if' scenarios" and none have focused on exploring the impact of multiple strategies on resilience. According to Kamalahmadi and Parast (2016), one research gap is how firms can choose between different strategies using analytical tools and how the level of resilience of a system can be defined quantitatively. This chapter aims to develop a concept that combines quantitative and qualitative resilience elements in order to calculate a score for supply chain resilience. With such a concept, it could be possible to compare supply chains and companies with regard to their resilience level.

2 Supply Chain Resilience

The high number of sources of complexity exposes the network to an increasing level of uncertainty, and the uncertainty level exposes the network to numerous kinds of events creating a potential for unpredictable disruptions (Güller et al. 2015). The occurrence of these events is usually random and has a probability of occurrence because not every future event or circumstance can be predicted. Even if the best forecasting methods are used, there will always be a certain degree of uncertainty. Zsidisin (2003) gives a suitable definition for the term "risk" in the supply chain context as "the potential occurrence of an incident associated with inbound supply from individual supplier failures or the supply market, in which its outcomes result in the inability of the purchasing firm to meet customer demand or cause threats to customer life and safety." Managing uncertainties leading to risks is always a challenge that requires the ability to survive and adapt in the face of turbulent change. Hence, risk management has become an essential part of management decision and control in supply chains. Another way to respond to such major supply chain disruptions is to build a resilient supply chain. In the supply chain literature, resilience is essentially defined as the ability of a system to return to its original state or move to a new, more desirable state after being disturbed (Christopher and Peck 2004). More recently, Ponomarov and Holcomb (2009) define resilience as "the adaptive capability of the supply chain to prepare for unexpected events, respond to disruptions, and recover from them by maintaining continuity of operations at desired levels of connectedness and control over structure and function." In contrast to prior perception, their definition includes the aspect of preparation. According to Klibi (2010), the concept of resilience also implies the avoidance of threatening disturbances. Hohenstein et al. (2015) found 46 different definitions in their systematic literature review. A few of them are:

- "The ability of a system to return to its original state or move to a new, more desirable state after being disturbed" (Christopher and Peck 2004).
- "Resilience ensures that the supply chain can recover quickly and cost-effectively from disruptions caused by natural disasters (such as earthquakes), social factors (employee strikes), medical emergencies (epidemics such as H1N1 flu), economic setbacks (the bankruptcy of a critical link in the chain) or technological failures (a software crisis)" (Melnyk et al. 2014).
- "Supply chain resilience is concerned with the system's ability to return to its original state or to a new, more desirable, one after experiencing a disturbance, and avoiding the occurrence of failure modes" (Carvalho et al. 2012).
- "Resilience [...] focuses on the ability of the firm to sustain operation and recovery quickly in the face of a disruption" (Schmitt and Singh 2012).
- "Resilience—the ability to survive, adapt, and grow in the face of turbulent change" (Petit et al. 2013).
- "A supply chain can [...] be resilient if its original stable situation is sustained or if a new stable situation is achieved. In this research, resilience is understood as the ability of a supply chain to cope with change" (Wieland and Wallenburg 2013).

In the supply chain literature, several terms are linked with resilience, such as agility, flexibility, and robustness. These terms either complement the topic of resilience or are used interchangeably with it. For example, some researchers argue that robustness is part of a successful implementation of resilience, whereas others state that these two terms represent two different concepts. Christopher and Peck (2004) and Mandal (2012) state that resilience and robustness are terms used interchangeably in practice. A robust system has the ability to absorb a disturbance while retaining the same previous state, whereas a resilient system has the ability to adapt and achieve a new stable state (Asbjornslett 2008). This leads to the conclusion that robustness may be desirable but is not synonymous with a resilient supply chain. Sheffi (2004) emphasizes that supply chain agility is the ability to respond to unanticipated changes. According to Swafford et al. (2006), agility is defined as the supply chain's capability to respond quickly to short-term changes in demand (or supply) and environment. Most research articles of the existing literature claim that speed and flexibility are two important components of the supply chain agility. The concepts of flexibility and agility are therefore tightly coupled with supply chain resilience (Güller et al. 2015). Wieland and Wallenburg (2013) define resilience with two dimensions: agility, resulting from visibility and speed, and robustness, resulting from anticipation and preparedness. Christopher and Peck (2004) define agility as the third element of supply chain resilience. According to Longo and Ören (2008), the most important elements affecting supply chain resilience are: flexibility, agility, velocity, visibility, and redundancy. Based on the literature review, Lotfi et al. (2013) illustrate some overlapping and non-overlapping practices/initiatives across robustness, agility, and resilience. Consequently, resilience can be achieved through robustness, flexibility, and agility. In the context of robustness, redundant capacity is installed. It is an additional capacity that would be used to replace the capacity loss caused by a disruption. In this regard, flexibility entails redeploying previously committed capacity (Rice and Caniato 2003). On the other hand, instead of being prepared for every situation by creating a robust supply chain, it is much more appreciated to increase the flexibility of the supply chain to adapt quickly and efficiently to changes.

The process of a disruption can be categorized in different phases, as illustrated in Fig. 1. As disruptions may or may not occur, firms can take measures before and after an unforeseeable event in order to be resilient. Thus, according to Melnyk et al. (2014), actions that aim to avoid shocks or to be prepared for them are referred to as "resistance capacity," whereas "recovery capacity" is the ability to restore operations after a disruption has occurred. The difference between the two elements of "resistance" is that one refers to preventing disruptions entirely (avoidance) and the other to shortening the time between the start of a disruption and the beginning of the recovery process (containment). The recovery process, in turn, consists of a "stabilization" phase and the "return" to a steady-state performance. The length of stabilization depends on the severity of the disruption. Ponomarov and Holcomb (2009) identify one more phase of supply chain resilience besides resistance and recovery, which is called the response phase. During this phase, a supply chain develops the ability to learn and adapt in response to disturbances. This diagram helps to visualize the magnitude of disturbance impact on the system performance.

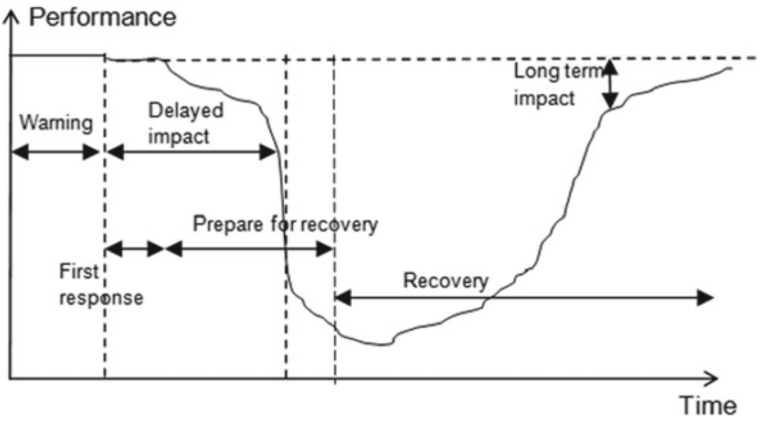


Fig. 1 Different phases of a disruption based on Sheffi (2004)

3 Elements of Supply Chain Resilience

In order to understand resilience in supply chains, it is crucial to analyze existing factors that help build resilience. In the current literature, there are many terms for "elements" that are used to achieve resilience. Longo and Ören (2008) use the term elements, whereas Ponomarrow and Holcomb (2009) as well as Scholten et al. (2014) call them antecedents and Soni et al. (2014) use the term enablers (Longo and Ören 2008; Ponomarov and Holcomb 2009). The term capability is used by other authors (Fiksel et al. 2015; Petit et al. 2012).

For instance, Blackhurst et al. (2005) name three elements that manage supply chain disruptions: "disruption discovery," "disruption recovery," and "supply chain redesign." Thus, "discovery" is a capability that is required before the disruption takes place. "Recovery" and "redesign" are essential elements in the time after the disruption occurrence.

Resiliency criteria are used to quantify different aspects of the supply chain resilience (SCRES). The decision support framework for SCRES by Falasca et al. (2008) consists of three major criteria. These are SC density, SC complexity, and the number of critical nodes in an SC. The SC density is defined as "the quantity and geographical spacing of nodes within a supply chain." The second determinant (SC complexity) is defined as the number of nodes and interconnections between the nodes in an SC. Therefore, a highly complex SC has plenty of nodes and plenty of interconnections between these nodes. The number of critical nodes in an SC is the third determinant and defines specific nodes within an SC and the relative importance of it. Regarding SCR, the connection between these three determinants is described as complex (Falasca et al. 2008).

The elements discussed by Ponomarov and Holcomb (2009) are: agility, responsiveness; visibility; flexibility/redundancy; structure and knowledge; reduction of uncertainty, complexity, reengineering; collaboration; integration, operational capabilities, and transparency. For agility and responsiveness, as well as visibility, the explanations of Christopher and Peck (2004) are used again. Flexibility is again determined as the ability of a company to quickly respond to changed market conditions, but there is also a connection made between redundancy and flexibility.

Petit et al. (2013) created a "supply chain resilience framework" which defines seven vulnerability factors. These vulnerability factors are considered to be the source of changes and are divided into 40 sub-factors. To counter the vulnerability factors, 14 managerial capability factors with 71 sub-factors are introduced. It is important to balance the vulnerabilities and the capabilities because if an SC has a high capability but only a low vulnerability, the profits of an SC erode. On the other hand, if the vulnerability is high but the capability is low, the SC has a high exposure to risks.

Cardoso et al. (2014) developed a "mixed integer linear model" to assess the SCRES. The latest model published in 2015 consists of eleven criteria to measure SCRES which are introduced as indicators. The economic performance is measured in terms of the expected net present value (ENPV). The eleven criteria are divided into three different categories. The first category is "network design indicators" with four criteria and the second category is "network centralization indicators" (Cardoso et al. 2015) also with four criteria. The last category is defined as "operational indicators" and consists of three criteria. The categories network design indicators and network centralization indicators are assessed in contrast to the operational indicators. To test the presented criteria, the authors applied the model to five existing supply chains which all have different designs. They conclude that SCs with a resilient design from the beginning need less mitigation strategies to handle disruptions. Additionally, to measure if an SC is resilient, a decision-making process and a large variety of different scenarios need to be implemented and assessed using simulations (Cardoso et al. 2015).

Soni et al. (2014) identified 14 elements forming supply chain resilience: agility, collaboration, visibility, risk management culture, adaptive capability, risk and revenue sharing, trust among players, information sharing, sustainability, corporate social responsibility, information security, supply chain structure, strategic risk planning, and knowledge sharing. The authors propose graph theory can be used to measure SC resilience. Sustainability is a key enabler for resilience of supply chains because improved understanding of what constitutes sustainability in a supply chain helps managers make better decisions. Hence, the risks of a single company and the whole supply chain are decreased. Risk and revenue sharing enables collaboration between supply chain members and makes it possible to focus on long-term decisions. Sharing benefits with upstream and downstream partners allows the sharing of risks, thus creating a competitive advantage. A precondition for this risk and revenue sharing is trust among the players. Trust diminishes functional conflict, allows greater cooperation, and improves integration and decision-making under uncertain conditions. On the other hand, a lack of trust contributes to supply chain risks. In this context, trust is defined as the expectation that no supply chain partner will act in an opportunistic way, although it might show advantages in the short term. Therefore, trust presents itself as very important for the long-term stability of an organization and its supply chain. In addition, it makes cooperation and collaboration possible within the organization and with partners.

Scholten et al. (2014) adopt the four elements introduced by Christopher and Peck (2004): supply chain (re)engineering, collaboration, agility, and risk awareness. Additionally, they consider risk awareness/knowledge management as a fifth system-level element. A supportive management culture and direct top management support are needed to establish a resilient supply chain. A part of this is the capacity to learn from past disruptions to improve preparedness for future events. A measure for this can be training for employees, suppliers, and customers about security and supply network risks to raise awareness and reinforce the importance of supply chain resilience.

4 A Framework for Resilience Assessment in Supply Networks

After analyzing the existing literature for core elements and measurement approaches to supply network resilience, this section provides a concept for resilience assessment. The presented measurement in the previous section has foundations that are either quantitative, like Spiegler et al. (2012), or qualitative like Petit et al. (2012). The developed concept combines both; some sub-factors can be calculated quantitatively, whereas others cannot. The main framework for resilience assessment is presented in Fig. 2. In order to assign points for each sub-factor, scorecards are developed in the following section. Ratings are either quantitative when possible or qualitative when respectively subjective.

4.1 Supply Chain Design

The first factor in the category of interorganizational elements is "supply chain design." Supply chain complexity, density, and node criticality are identified as significant elements of resilience. Supply chain density and node criticality each have two measures. Hence, five sub-factors are taken into account for the assessment of supply chain resilience (SCRES) regarding the supply chain design.

4.1.1 Supply Chain Density (Average Internode Distance, Number of Critical Nodes)

A dense supply chain is more vulnerable to disruptions than a less dense network. Two measures for assessing the density of a supply chain are average internode distance and number of node areas (Craighead et al. 2007). In this regard, both are

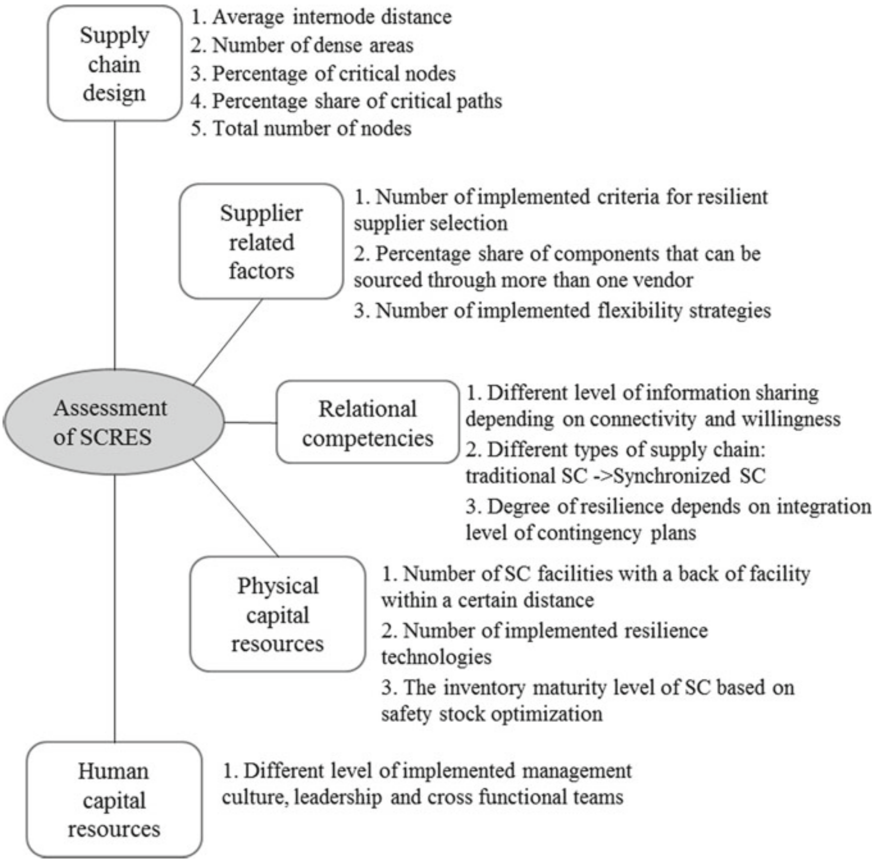


Fig. 2 Summary of approaches for the evaluation of each sub-factor

considered sub-factors. First, for calculating the average internode distance $d_{\emptyset}$, the distances $d(n_{Pi})$ of all pair of nodes n_P have to be added together:

$$d = \sum_{i=1}^{n_{Pi}} d(n_{Pi}), i = 1 \rightarrow n_P$$

Second, to get the average internode distance $d_{\emptyset}$, the overall distance d has to be divided by the number of all pair of nodes n_P:

$$d_{\emptyset} = \frac{d}{n_P}$$

The second suggestion of Craighead et al. (2007) is the number of node areas within a supply chain. On first sight, it seems redundant to use both the density average internode distance and number of dense areas. For example, a supply network with a relatively high-average internode distance is said to be more resilient than a comparable network with a lower-average internode distance, as the latter is denser. However, the structure of both supply chains has to be considered. The former can consist of a few very dense areas that are geographically far away from each other. The high distances between the areas increase the average internode distance, making the supply chain less dense, when considering the entire network. But the existence of many dense areas decreases resilience, and thus, in terms of supply chain design, the supply chain with a higher-average internode distance is not necessarily more resilient than the more balanced supply chain with a lower-average internode distance.

When describing a supply chain through the number of dense areas within it, all the criteria for dense areas have to be defined. Craighead et al. (2007) mention “when entities within a supply chain reside in close proximity to one another within a geographical region, that specific portion of the supply chain (i.e., that region) can be deemed to be densely populated.” Yet, this might not be sufficient for quantitatively assessing the number of dense areas and for further use of it as a sub-factor for measuring SC resilience (SCRES). Either there are clearly defined characteristics or there is a way of calculating whether an area can be considered dense or not. Unfortunately, the current supply chain management literature does not offer a definition for a dense area.

To evaluate the average internode distance and transfer it into the appropriate number of points on the scale from 1 to 5, a respective correlation is needed. Accordingly, “1” means a very low contribution to SCRES (very low-average internode distance). Contrastingly, “5” is very good regarding resilience, as denser supply chain networks are more vulnerable to disruptions. Table 1 shows the scorecard for this sub-factor.

For the sub-factor “number of dense areas within the supply chain,” a score of 5 means that no dense areas exist in the supply chain network, which increases resilience. Conversely “1” stands for many dense areas that affect SCRES negatively (see Table 2).

The problems with these two sub-factors are evident. Firstly, it lacks a definition for a “dense area” from a SCM perspective. Some parts of a supply chain are denser than others, but specific characteristics are missing. Secondly, even though average internode distance and number of dense areas can be calculated in a quantitative manner, indicators for each of the two sub-factors are not sufficient to establish what

Table 1 Scorecard for internode distance

Score	Internode distance
1	Very low-average internode distance
2	Low-average internode distance
3	Moderate internode distance
4	High internode distance
5	Very high internode distance

Table 2 Scorecard for number of dense areas

Score	Number of dense areas
1	Many dense areas exist within the supply chain
2	Several dense areas exist within the supply chain
3	Few dense areas exist within the supply chain
4	One dense area exists within the supply chain
5	No dense areas exist within the supply chain

is, or is not, resilient. Hence, the scorecards do not give exact figures for the distance and the number of dense areas.

4.1.2 Node Criticality (Number of Critical Nodes, Number of Critical Paths)

The more important node or the path between two nodes is more critical for the resilience of the supply chain. Such critical nodes and paths decrease SCRES directly (Blackhurst et al. 2005; Craighead et al. 2007). To quantify this, distinct sub-factor traits are essential. Following Christopher and Peck (2004), the four characteristics of critical paths can be used to count the number of critical connections between nodes and nodes themselves.

The absolute number of both critical nodes and paths is not very insightful, as it strongly depends on the size of the considered supply network. For instance, the same number of critical nodes can be good for a long supply chain while indicating low resilience in a smaller network. The number of critical paths n_{pc} can be put in relation to all paths, which equal all pairs of nodes n_p, and critical nodes n_c in relation to the total number of nodes n. Correspondingly, the percentage share of critical paths $cp_{\%}$ and the percentage share of critical nodes $cn_{\%}$ are calculated as follows:

$$cp_{\%} = \frac{n_{pc}}{n_p} \times 100; \quad cn_{\%} = \frac{n_c}{n} \times 100$$

In line with this, $cp_{\%}$ and $cn_{\%}$ can be used as measures for the sub-factor node and path criticalities. High percentage shares of critical paths and nodes imply more potential vulnerabilities in a supply chain, and consequently lower resilience, as illustrated in Tables 3 and 4.

As with the first two sub-factors, “number of critical nodes” and “number of critical paths” can be calculated in a simple way. Determining the percentage share of critical nodes/paths that relates to the lowest resilience score is the main challenge. In fact, the assessment of both sub-factors based on the estimation that $cp/n_{\%} \geq 15\%$ is rated as the lowest contribution to SCRES.

Table 3 Scorecard for critical nodes

Score	$cn_{\%}$
1	$cn_{\%} \geq 15\%$
2	$15\% > cn_{\%} \geq 10\%$
3	$10\% > cn_{\%} \geq 5\%$
4	$5\% > cn_{\%} \geq 0\%$
5	0%

Table 4 Scorecard for critical paths

Score	$cp_{\%}$
1	$cp_{\%} \geq 15\%$
2	$15\% > cp_{\%} \geq 10\%$
3	$10\% > cp_{\%} \geq 5\%$
4	$5\% > cp_{\%} \geq 0\%$
5	0%

4.1.3 Supply Chain Complexity

Within the scope of this paper, supply chain complexity is only considered from a design perspective. Serdar-Asan (2013) distinguishes between three different types of supply chain complexity: static, dynamic, and decision-making. Interestingly, complexity concerning the supply chain structure is of a static nature. Dynamic complexity involves uncertainty, and decision-making combines both types. Craighead et al. (2007) suggest that supply chain complexity can simply be measured by summing up the total number of nodes and flows.

On first sight, it seems difficult to assess supply chain complexity accurately in this way, in the case of just one contemplated supply chain. However, this works well when comparing two similar large supply chains in order to determine which one is more complex. Still, this relatively simple way is a useful approach for measuring the sub-factor supply chain complexity. Naturally, larger supply networks would have more nodes and flows, which in fact makes them less resilient. Thus, following Craighead et al., complexity, c, is the sum of all nodes, n, and all flows, which are categorized into forward flows $f_{forward}$, backward flows $f_{backward}$, and within-tier flows $f_{within-tier}$.

$$c = n + f_{forward} + f_{backward} + f_{within-tier}$$

Consequently, the result for c indicates how resilient a company's supply chain is in terms of its network structure. According to this, firms with smaller breadth supply chains would have a higher score for this sub-factor, by default. This is actually correct, because small supply chains with less nodes and flows are less likely to be affected by a disruption. Table 5 shows the scores for the respective number of nodes and flows.

Table 5 Scorecard for supply chain complexity

Score	c
1	c ≥ 500
2	$500 > c \geq 350$
3	$350 > c \geq 250$
4	$250 > c \geq 150$
5	c < 150

Table 6 Criteria for resilient suppliers

Criteria	Description
Catastrophic risk exposure	Applies when the probability of natural hazards is low and not likely to affect the supplier's site
Audit of risk profile	Applies when the supplier audits its own risk profile regularly
Monitoring and mitigation of risks	Applies when the supplier monitors and mitigates risks regularly
Supply chain continuity management	Applies when the supplier has established a supply chain continuity management system

4.2 Supplier-Related Factors

Supplier-related factors are part of the interorganizational category of SCRES elements. They include supplier selection, multiple sourcing, and flexibility in sourcing.

4.2.1 Supplier Selection

Risk-related factors are the key criteria in a resilience context with regard to supplier selection (Christopher and Peck 2004). General risk factors of a supply chain location can be the geographical location, political stability, or the economic position (Chen et al. 2014). Mitigation of such risks is the aim of SCRM rather than SCRES. In terms of resilience, unexpected disasters are of bigger importance. Thus, the "catastrophic risk exposure" (Knemeyer et al. 2009), which depends on the geographical location, is the first of four criteria. Consequently, it needs to be evaluated if the site of the vendor is exposed to catastrophic risks like earthquakes or floods. The remaining three factors concern the risk awareness of the supplier. Christopher and Peck (2004) propose "audit of own supply chain risk profile" and "procedures for monitoring and mitigation of risks" as the main criteria. Adding "supply chain continuity management," which is crucial for resilient supplier selection according to Rajesh and Ravi (2015), four criteria are identified (see Table 6).

A resilient supplier selection requires all of these criteria. This means that if a particular supplier does not meet all four criteria, that firm should not be selected as a supplier. The score for this sub-factor depends on how many of the criteria are

Table 7 Scorecard for supplier selection

Score	Number of positive criteria
1	0 criteria positive
2	1 criterion positive
3	2 criteria positive
4	3 criteria positive
5	4 criteria positive

utilized in the supplier selection process of the considered firm. Correspondingly, if none is taken into account, it means a score of 1, and if all are used, then the score is 5. Thus, the assessment of the sub-factor "supplier selection" is based on relevant selection criteria with regard to resilience. The score does not depend on how many of the suppliers fulfill the respective criteria. As a matter of fact, a resilient supplier should fulfill all of the identified characteristics. The selection criteria of the considered company are the determining variable, although in the current state of research there are no quantitative measures for the identified criteria (Table 7).

4.2.2 Multiple Sourcing

There are various ways of measuring the sub-factor "multiple sourcing." Despite cost and quality disadvantages, having more than one supplier for a specific component will always reduce the effect of a supply chain disruption, at least to a small extent. Still, it is not clear that the more sources a firm uses, the more resilient it is with its sourcing strategy. For example, one could take the total number of suppliers in relation to the quantity of components in order to determine the resilience degree of a company. This could be an indicator, but it does not reveal anything about the allocation of suppliers of the various components. Another way of assessing a company's degree of "multiple sourcing" is to count how many components are being procured through more than one supplier. The number of suppliers for each component is not taken into account, meaning that having five different suppliers for an individual part has the same influence on the score as having just two. Nonetheless, this simple calculation provides a lot of information about this particular sub-factor. Consequently, the percentage share $ms_{\%}$ of parts that are obtained by multiple sourcing is calculated by dividing all components that are, or at least could be, procured through more than one vendor $p_{multiple\,sources}$ by all components p.

$$ms_{\%} = \frac{p_{multiple\,sources}}{p} \times 100$$

Following this, a percentage share of 100% means the highest degree of resilience and five points according to the scorecard. In contrast, 0% corresponds to one point (see Table 8). The numbers for each score follow a consistent segmentation of the percentage share.

Table 8 Scorecard for multiple sourcing

Score	$ms_{\%}$
1	$ms_{\%} < 20\%$
2	$40\% > ms_{\%} \geq 20\%$
3	$60\% > ms_{\%} \geq 40\%$
4	$80\% > ms_{\%} \geq 60\%$
5	$100\% > ms_{\%} \geq 80\%$

4.2.3 Flexibility in Sourcing

Although many authors in the field of supply chain resilience see multiple sourcing and sourcing flexibility as the same thing, like Pereira et al. (2014), these sub-factors are treated separately in the scope of this paper. According to Petit et al., multiple suppliers are part of "flexibility in sourcing." Thus, using multiple vendors enables flexibility. Even so, sourcing flexibility has many aspects that play a role in terms of SCRES. Petit et al. (2013) define six different sub-factors for "flexibility in sourcing," which is one of their fourteen capability factors: part commonality, modular product design, multiple uses, supplier contract flexibility, multiple sources.

These sub-factors are conceivable to assess a supply chain's capability of "sourcing flexibility." It would include determining how many of the identified flexibility factors are used by the contemplated firm. The more strategies that are implemented, the higher the respective score. Transferred to the scorecard, the implementation of all six flexibility strategies equals five points. As five factors are taken into account, one or zero used techniques mean zero points (see Table 9).

The obvious difficulty is that the awarding of scores is still based on qualitative evaluations. It needs to be decided if, for example, part commonality or modular product design is given in the object of study. Clear definitions are needed in order to determine if a company makes use of a specific strategy or not. As far as multiple sourcing is concerned, the percentage share of multiple sourcing $ms_{\%}$ can be used as an indicator, defining that starting from a specific share, for instance $ms_{\%} = 75\%$, this sub-factor is "positive." Similar measures or indicators are necessary for the other sub-factors as well.

The second problem concerns mainly modular product design. The implementation of this strategy depends on the characteristics of the outcome. Despite its

Table 9 Scorecard for flexibility in sourcing

Score	Description
1	0 or 1 strategy
2	2 strategies
3	3 strategies
4	4 strategies
5	5 strategies

Table 10 Measures for connectivity and willingness (Allred et al. 2009)

Measures for connectivity	Measures for willingness
Integration of information applications in the firm and the supply chain	Willingness to share information among supply chain members
Existence of information system linkages with suppliers and customers	
	Frequency of information sharing among supply chain members
	Existence of senior-level managerial interaction among supply chain members

advantages, modular product design is not always suggestive or even possible. In that case, it cannot be considered for the assessment of "flexibility in sourcing."

4.3 Relational Competencies

The factor of relational competencies consists of three sub-factors: information sharing, collaboration, and contingency planning. The central aspects of information sharing are the two proposed dimensions of connectivity and willingness. In fact, one does not work without the other. If a company has sufficient information sharing systems and technology but is not willing to make use of them, the contribution to resilience is low and vice versa. Firms that want to communicate with suppliers and customers but lack the necessary infrastructure do not have a high level of information sharing.

Hence, a measurement tool for information sharing does not exist, but it is possible to assess the extent of information sharing in a particular firm or supply chain. The following approach to assess the sub-factor of relational competencies is based on different levels of communication. Altogether, five measures for the dimensions of connectivity and willingness are adopted from Allred et al. (2009).

According to the five-point rating scale, five levels of information sharing determine the contribution to SCRES, which are characterized by the measures in Table 10. As explained, willingness alone cannot enable communication in supply chains. Information applications and systems are inalienable requirements. While the score 1 is the absence of these measures, the score 5 includes an appropriate implementation of all measures (see Table 11).

4.3.1 Collaboration

The coherence between information sharing and collaboration is not clearly established. Although definitions of supply chain collaboration are not consistent, the

Table 11 Scorecard for information sharing

Score	Description
1	(1) No information applications are integrated into the firm and the supply chain, and (2) no information system linkages exist with suppliers and customers
2	(1) Information applications are integrated into the firm and the supply chain, and (2) information system linkages exist with suppliers and customers but (3) low willingness to share information among supply chain members
3	(1) Information applications are integrated into the firm and the supply chain, and (2) information system linkages exist with suppliers and customers as well as (4) occasional information sharing among supply chain members
4	(1) Information applications are integrated into the firm and the supply chain, and (2) information system linkages exist with suppliers and customers as well as (4) frequent open information sharing among supply chain members
5	(1) Information applications are integrated into the firm and the supply chain, and (2) information system linkages exist with suppliers and customers as well as (4) frequent open information sharing and (5) senior-level managerial interaction among supply chain members

aim is unambiguous: Collaboration is supposed to lead to transparency and visibility (Holweg et al. 2005).

There are several collaboration initiatives such as vendor-managed inventory (VMI), efficient consumer response (ECR), collaborative planning, forecasting, and replenishment (CPFR), and continuous replenishment (CR) (Ireland and Crum 2005). A possible approach to assessing a company's collaboration capability could be to gather the most common initiatives in order to detect how many of them are implemented, similar to the assessment of "flexibility in sourcing." The more identified initiatives that are used, the higher the visibility, thus a higher score and more resilience.

Holweg et al. (2005) distinguish between four different types of supply chains by means of collaboration. Planning collaboration and inventory collaboration are the crucial dimensions. The first type is referred to as the "traditional supply chain," which means that neither upstream nor downstream tiers collaborate. It is followed by the "information exchange" supply chain. Retailer and supplier exchange demand information as well as action plans and thus align their forecasts. In the "vendor-managed replenishment" supply chain, the supplier is responsible for managing the customer's inventory. Finally, in the last type, the supply is synchronized, which means that the supplier takes replenishment into account for his own production and material planning.

In order to use this classification as the foundation for the assessment of the sub-factor "collaboration," a fifth supply chain level needs to be added: The "pre-collaborative supply chain" is between the first and second type. No information is shared in the "traditional supply chain," and information is actively exchanged in the "information exchange supply chain." Thus, the "pre-collaborative supply chain" is characterized by a state where the issue of collaboration is understood and first efforts to collaborate were undertaken. However, unlike the second type, according

Table 12 Scorecard for collaboration

Score	Description
1	"Traditional supply chain"—with no collaboration
2	"Pre-collaborative supply chain"—no collaboration structures established yet
3	"Information exchange supply chain"—alignment of forecasts
4	"Vendor-managed replenishment"—supplier responsible for customer's inventory
5	"Synchronized supply chain"—supplier's production and material planning are aligned with replenishment

Table 13 Scorecard for contingency planning

Score	Description
1	No contingency plans
2	Contingency plans exist for single functional areas
3	Contingency plans exist for single sites
4	Customer and supplier are integrated into contingency plans
5	The entire supply chain is integrated into contingency plans

to Holweg et al. (2005), adequate structures and technology are not established yet. Table 12 shows the scorecard for this sub-factor with the four adopted and one added "collaboration levels."

4.3.2 Contingency Planning

Contingency planning is one way of increasing resilience. With the fast-changing business environment and many new risks, organizations are forced to develop plans that facilitate a fast response to disruptions. The cornerstone of contingency planning does not concern the mere existence of such plans. Skipper and Hanna (2009) state contingency planning is not yet a multi-organizational function, as it is often implemented around single functional areas only. It can be concluded that contingency plans, which are integrated on a supply chain network level instead of single departments, are more conducive to SCRES. This is a starting point for the assessment of the sub-factor "contingency planning." Thus, the integration level of contingency planning, from no plans at all to contingency plans that include all parts of a supply chain, determines the capability score regarding this sub-factor as shown in Table 13.

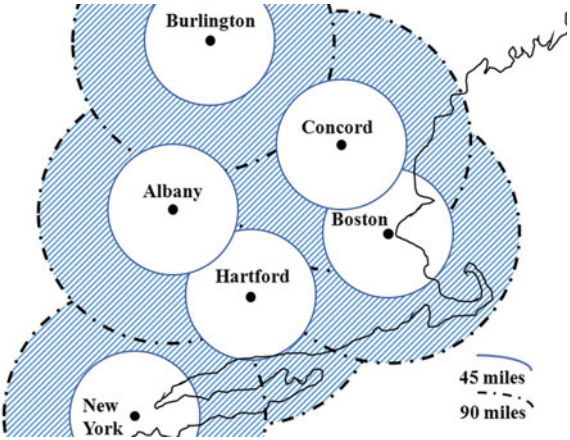


Fig. 3 Areas for the location of secure backup facilities based on Ratick et al. (2008, p. 648)

4.4 Physical Capital Resources

4.4.1 Backup Facilities

Day-to-day operational costs and costs of expected failure, as well as probability of an event occurrence, are decisive for the number and location of such facilities. Sites that are physically too close together can be affected by the same disaster, which causes a disruption, but if they are located too far apart, operations can become economically infeasible (Ratick et al. 2008). Following this basic principle, Hale and Moberg (2005) discuss the optimal location for backup facilities. The objective is the "selection of a minimum number of emergency resource locations that provide logistics managers with quick access to critical resources while minimizing the total costs spent by the supply chain preparing for future crises" (Hale and Moberg 2005). Hence, they developed a four-step secure site decision process.

In order to measure the sub-factor "backup facilities," the approach of Hale and Moberg (2005) can be utilized. Each supply chain facility needs to have at least one backup site that contributes to a fast recovery after a disruption. These backup sites should be within a specified "cover" distance, *C*. As locations that are too close to each other can be subject to the same hazard, the "anticover" distance, *A,* is the second requirement for a safe backup facility (see Fig. 3) (Ratick et al. 2008). The scorecard for this sub-factor is based on the assumption that, in terms of backup facilities, a supply chain can be said to be resilient if each supply chain facility has at least one backup site within a distance according to the model of Hale and Moberg (2005). This is done by calculating the percentage share of facilities $bf_{\%}$ that meet this requirement. In order to do so, the number of supply chain facilities with an adequate backup site scf_{backup} needs to be divided by all supply chain facilities, scf.

$$bf_{\%} = \frac{scf_{backup}}{scf}$$

Table 14 Scorecard for backup facilities

Score	Description
1	$bf_{\%} < 20\%$
2	$40\% > bf_{\%} \geq 20\%$
3	$60\% > bf_{\%} \geq 40\%$
4	$80\% > bf_{\%} \geq 60\%$
5	$100\% > bf_{\%} \geq 80\%$

Table 15 Resilience enabling technologies based on Blackhurst et al. (2005), Prajogo and Olhager (2012)

Resilience enabling supply chain technologies
Exception reporting systems and predictive tools for early awareness of impending disruptions
Risk monitoring systems for each node of the supply chain
Tools for quickly redesigning the supply chain
Information systems to track/locate resources

The correlation according to the five-point rating scale (see Table 14) is similar to the one of the sub-factor "multiple sourcing."

The problem is that "cover" distance, *C,* and "anticover" distance, *A,* are not generally defined. Not every area of a supply chain is threatened by hazards to the same extent. Therefore, different regions and parts of a supply chain network need to be considered and assessed separately concerning the distances.

4.4.2 Technology

The sub-factor "technology" cannot be measured quantitatively. However, similar to "flexibility in sourcing," it can be assessed. The basis for this is the three technologies/tools identified by Blackhurst et al. (2005), shown in Table 15, and additionally a technology adopted from *Prajogo and Olhager*, which is "information systems to track/locate resources" (Prajogo and Olhager 2012). The four suggested technologies cover all the relevant domains that require increased visibility that are discussed as part of the sub-factors "information sharing" and "collaboration," apart from relational competencies. Remaining issues concern technologies that enhance predictability, monitoring, and redesigning the supply chain. The more technologies that are implemented by a firm/supply chain, the higher the resilience score is for this sub-factor (see Table 16).

4.4.3 Safety Stock

Despite the disadvantages, carrying safety stock is one of the most common strategies to buffer against supply risks (Giunipero and Eltantawy 2004). Yet, although it is

Table 16 Scorecard for technology

Score	Description
1	0 technologies implemented
2	1 technology implemented
3	2 technologies implemented
4	3 technologies implemented
5	4 technologies implemented

part of most of the resilience frameworks, none of the researchers analyze the precise extent of safety stock that is needed. Mostly, authors only refer to the mere presence of safety stock as an enabler of SCRES (Blackhurst et al. 2005; Giunipero and Eltantawy 2004; Hoheinstein et al. 2015). In line with this, the scorecard for the sub-factor "safety stock" in principle resembles the measurement of backup facilities. In fact, the particular degree of safety stock is not considered. Thonemann and Klein (2011) suggested five different maturity levels for inventory in supply chains. The scorecard for this sub-factor based on the inventory maturity level is shown in Table 17.

4.5 Human Capital Resources

Leadership, multi-disciplinary teams, and understanding of risk are identified as the core elements of SCRES regarding human capital resources. In order to measure these three sub-factors individually, a very detailed analysis is necessary. More than the other considered factors, human capital resources need to be viewed from a management perspective. A quantitative measurement seems impossible, as precise indicators or different levels have to be defined for each sub-factor, although using qualitative references, "human capital resources" can be assessed. Considering "human capital resources" as only one factor, the three sub-factors can be seen as different levels of the degree of resilience. Leadership in a resilience context is useless if a risk management culture is not existent. Similarly, multi-disciplinary teams that work in

Table 17 Scorecard for the sub-factor safety stock

Score	Inventory maturity level according to Thonemann and Klein (2011)
1	Same parameter is used to calculate the inventory target levels for all products
2	Individual stock parameters are applied, based on the planners' experience
3	Individual stock parameters are applied to each product segment
4	Analytical optimization models for the determination of safety stock levels are applied—single-stage inventory optimization
5	Multistage approaches for the joint planning and optimization of inventory levels throughout the supply chain are applied

Table 18 Scorecard for human capital resources

Score	Description
1	Risk management culture does not exist, and fundamental assumptions are not yet understood
2	Risk management culture exists but is not yet internalized by all employees
3	Risk management culture is internalized by all employees, and cost/benefit trade-offs when managing risk in supply chains are understood
4	Employees are educated and trained to execute supply chain contingency plans, and leaders are present
5	Cross-functional risk management teams are established

order to monitor risks and predict possible threats cannot function effectively if the employees involved lack of essential understanding of the issue.

To classify a company's resilience ability regarding human capital resources, at least five different levels need to be defined. "Education and training of employees to execute supply chain contingency plans" and "understanding of cost/benefit trade-offs when managing risk in supply chain" are two identified resilience enhancers in terms of human capital resources by Blackhurst et al. (2011). Adopting these two, the corresponding scorecard (Table 18) looks as follows.

4.6 *Overall Resilience Score*

The respective scores of all the sub-factors contribute to the capability of a company or supply chain to be resilient. The overall resilience score R is calculated as follows:

$$R = \frac{C}{5}$$

The resilience capability C is calculated by averaging the five factor scores $C_{1,2,3,4,5}$:

$$C = \frac{\sum_{j=1}^{n_C} C_j}{n_C}, n_C = 5$$

The factor scores C_j are averaged from the respective sub-factors $C_{j,k}$ (see Table 19):

$$C_j = \frac{\sum_{k=1}^{n_{C_j}} C_{j,k}}{n_{C_j}}, j = 1 \rightarrow n_C$$

Three different ways of determining the score for the sub-factors are used: Sub-factors that can be quantified have a scorecard with a ranking system according to the

Table 19 Overview resilience factors and sub-factors

Resilience factors C_j	Sub-factors $C_{j,k}$
Supply chain design	(1) Average internode distance, (2) number of dense areas, (3) number of critical paths, (4) number of critical nodes, (5) supply chain complexity
Supplier-related factors	(1) Supplier selection, (2) multiple sourcing, (3) flexibility in sourcing
Relational competencies	(1) Information sharing, (2) collaboration, (3) contingency planning
Physical capital resources	(1) Backup facilities, (2) technology, (3) safety stock
Human capital resources	(1) Human capital resources

respective measure, for example “average internode distance.” For sub-factors that cannot be quantified, qualitative indicators are utilized. These can be certain characteristics that concern the related sub-factor, for example “human capital resources,” or different strategies or criteria, for instance “technology,” that help to determine the score. However, no matter how detailed and well described the qualitative indicators are, the assessment of several sub-factors remains subjective to a certain extent. “Information sharing” is a good example of that: Even though the scorecard says clearly which requirements correspond to which score, these still need to be evaluated. The correlation between the factors and sub-factors is not part of the measurement concept. All sub-factors are considered individually. This, and the assumption of equal weights for all factors, based on Petit et al. (2013), allows the calculation of the resilience score in a simple manner. In order to determine the weight for each factor and validate the developed concept, an empirical study is needed. Another main issue is to compare results between different resilience scores and quantify the quality of resilience index. Petit et al. (2013) suggest utilizing the five-point Likert to identify the resilience index and assume equal weights for each factor.

5 Conclusion and Future Research

As SCRES research is relatively novel and not well researched to date, the aim of this chapter is to develop a concept for assessing supply chain resilience. Compared to the high number of distinct resilience concepts, the proposed definitions differ slightly. A detailed analysis of the roots of resilience as well as its phases and formative elements is a vital process step in order to develop a concept for assessing SCRES. As demonstrated in this chapter, resilience is composed of many different competencies. Therefore, it is often considered a concept or strategy rather than a certain capability of a supply network. To summarize, the study revealed two main difficulties in the development of a concept for measuring SCRES. The first one relates to finding quantitative numbers or indices for the particular sub-factors. Unfortunately, this simply cannot be done for some factors, for example “relational competencies” or “human capital resources.” However, specifically concerning supply chain design factors, appropriate measures can be calculated and implemented in the concept. If this is not possible, qualitative indicators need to be established.

The second issue concerns the correlation between known measures/indicators, quantitative or qualitative, and the respective resilience scores. Even if the quantitative measurement of a certain sub-factor is possible, there is no evidence for how it correlates with the five-point ranking scale. As research in this field is not yet sufficiently advanced, the corresponding scorecards are sometimes still based on subjective estimations. The same holds true for qualitative measures.

Another issue relating to the development of the concept concerns contradictions. This is clarified when considering, for example, the two sub-factors of “multiple sourcing” and “supply chain complexity.” Multiple sourcing is a resilience enabler, while supply chain complexity reduces resilience. However, each additional source adds a redundant path, which increases complexity. As a matter of fact, a supplementary supplier increases and diminishes resilience at the same time.

Companies need a structured, methodical, and incremental approach for implementing SCRES holistically. In the course of this, the enablers of resilience need to be considered as a whole. A well-defined procedure is necessary because the implementation of some elements is conditional to the existence of certain structures. This means that there might be a chronological order for building resilience, which needs to be explored in the future. Furthermore, supply chains have different characteristics due to the demands of different industries. These circumstances need to be taken into account for effective implementation.

The cost/benefit trade-off is vital and determines if actions that were taken to achieve resilience were advisable. Although often mentioned in the specialized literature, there is a lack of any detailed analysis. If investments in resilience are too low, the vulnerability of the supply chain is too high. At the same time, profits will erode if companies do not balance their efforts. This compromise between additional costs and use of resilience-related actions needs to be quantified in the future. Obviously, having a valid tool to measure SCRES in a quantitative way is a necessary requirement. Such a tool can be based on the concept for assessing supply chain resilience developed here and, in addition, integrate the importance and interrelations of resilience elements.

References

Allred, C., Wallin, C., Magnan, G., & Fawcett, S. E. (2009). Supply chain information-sharing: Benchmarking a proven path. *Benchmarking: An International Journal*, *19*(2), 222–246.

Asbjørnslett, B. (2008). Assessing the vulnerability of supply chains. In G. A. Zsidisin & B. Ritchie (Eds.), *Supply chain risk: A handbook of assessment, management and performance* (pp. 15–33). New York, NY: Springer.

Blackhurst, J., Craighead, C. W., Elkins, D., & Handfield, R. B. (2005). An empirically derived agenda of critical research issues for managing supply-chain disruptions. *International Journal of Production Research, 43*(19), 4067–4081.

Blackhurst, J., Dunn, K. S. & Craighead, C. W. (2011). An empirically derived framework of global supply resiliency. *Journal of business logistics, 32*(4), 374–391.

Cardoso, S., Barbosa, A. P. F. D., Relvas, S., & Novais, A. (2014). Resilience assessment of supply chains under different types of disruption. In *Proceedings of the 8th International Conference on Foundations of Computer-Aided Process Design* (pp. 759–764).

Cardoso, S., Barbosa, A. P. F. D., Relvas, S., & Novais, A. (2015). Resilience metrics in the assessment of complex supply-chains performance operating under demand uncertainty. *Omega, 56,* 53–73.

Carvalho, H., Barroso, A. P., Machado, V. H., Azevedo, S., & Cruz-Machado, V. (2012). Supply chain redesign for resilience using simulation. *Computers & Industrial Engineering, 62*(1), 329–341.

Chan, H., & Chan, F. (2010). Comparative study of adaptability and flexibility in distributed manufacturing supply chains. *Decision Support Systems, 48*(2), 331–341.

Chen, A., Hsieh, C. Y., & Wee, H. M. (2014). A resilient global supplier selection strategy—A case study of an automotive company. *The International Journal of Advanced Manufacturing Technology, 87*(5–8), 1475–1490.

Christopher, M., & Peck, H. (2004). Building the resilient supply chain. *International Journal of Logistics Management, 15*(2), 1–13.

Craighead, C. W., Blackhurst, J., Rungstusanatham, M. J., & Handfield, R. B. (2007). The severity of supply chain disruptions: Design characteristics and mitigation capabilities. *Decision Sciences, 38*(1), 131–156.

Falasca, M., Zobel, C. W., & Cook, D. (2008). A decision support framework to assess supply chain resilience. In *Proceedings of the 5th International ISCRAM Conference, Washington, DC, USA* (pp. 596–605).

Fiksel, J., Polyviou, M., Croxton, K. L., & Petit, T. J. (2015). From risk to resilience—Learning to deal with disruption. *MIT Sloan Management Review, 56*(2), 79–86.

Giunipero, L. C., & Eltantawy, R. A. (2004). Securing the upstream supply chain: A risk management approach. *International Journal of Physical Distribution & Logistics Management, 34*(9), 698–713.

Güller, M., et al. (2015). A simulation-based analysis of supply chain resilience. In W. Kersten, T. Blecker, & C. Ringle (Eds.), *Innovative methods in logistics and supply chain management* (pp. 533–557). Berlin: epubli GmbH.

Hale, T., & Moberg, C. R. (2005). Improving supply chain disaster preparedness: A decision process for secure site location. *International Journal of Physical Distribution & Logistics Management, 35*(3), 195–207.

Hoheinstein, N. O., Feisel, E., Hartmann, E., & Giunipero, L. (2015). Research on the phenomenon of supply chain resilience: A systematic review and paths for further investigation. *International Journal of Physical Distribution & Logistics, 45*(1–2), 90–117.

Holweg, M., Disney, S., Holmström, J., & Smaros, J. (2005). Supply chain collaboration: Making sense of the strategy continuum. *European Management Journal, 23*(2), 170–181.

Hongler, M., et al. (2010). Centralized versus decentralized control—A solvable stylized model in transportation. *Physica A, 389*(19), 4162–4171.

Ireland, R. K., & Crum, C. (2005). *Supply chain collaboration. How to implement CPFR and other best collaborative practices*. Boca Raton: J. Ross Publishing.

Jüttner, U. (2005). Supply chain risk management: Understanding the business requirements from a practitioner perspective. *The International Journal of Logistics Management, 16*(1), 120–141.

Kamalahmadi, M., & Parast, M. (2016). A review of the literature on the principles of enterprise and supply chain resilience: Major findings and directions for future research. *International Journal of Production Economics, 171*(1), 116–133.

Kleindorfer, P., & Saad, G. (2005). Managing disruption risks in supply chains. *Production and Operations Management, 14*(1), 53–68.

Klibi, W., Martel, A., & Guitouni, A. (2010). The design of robust value-creating supply chain networks: A critical review. *European Journal of Operations Research, 203*(2), 283–293.

Knemeyer, A. M., Zinn, W., & Eroglu, C. (2009). Proactive planning for catastrophic events in supply chains. *Journal of Operations Management, 27*(2), 141–153.
Longo, F., & Ören, T. (2008). *Supply chain vulnerability and resilience: A state of the art overview*. Italy: Campora S. Giovanni.
Lotfi, M., Sodhi, M., & Kocabasoglu-Hillmer, C. (2013). *How efforts to achieve resiliency fit with lean and agile practices*. USA: Denver.
Mandal, S. (2012). An empirical investigation into supply chain resilience. *Journal of Supply Chain Management, 9*(4), 46–61.
Manuj, I., & Mentzer, J. T. (2008). Global supply chain risk management strategies. *International Journal of Physical Distribution & Logistics Management, 38*(3), 192–223.
Melnyk, S. A., et al. (2014). Understanding supply chain resilience. *Supply Chain Management Review, 18*(1), 35–41.
Nair, A., Narasimhan, R., & Choi, T. (2009). Supply networks as a complex adaptive system: Toward simulation-based theory building on evolutionary decision making. *Decision Sciences, 40*(4), 783–815.
Pereira, C. R., Christopher, M., & Da Silva, A. L. (2014). Achieving supply chain resilience: The role of procurement. *Supply Chain Management: An International Journal, 19*(5–6), 626–642.
Petit, F., et al. (2012). Developing an index to assess the resilience of critical infrastructure. *International Journal of Risk Assessment and Management, 16*(1), 28–47.
Petit, T. J., Fiksel, J., & Croxton, K. L. (2013). Ensuring supply chain resilience: Development of a conceptual framework. *Journal of Business Logistics, 31*(1), 1–21.
Ponomarov, S., & Holcomb, M. (2009). Understanding the concept of supply chain resilience. *International Journal of Logistics Management, 20*(1), 124–143.
Prajogo, D., & Olhager, J. (2012). Supply chain integration and performance: The effects of long term relationships, information technology and sharing, and logistics integration. *International Journal of Production Economics, 135*(1), 514–522.
Rajesh, R., & Ravi, V. (2015). Supplier selection in resilient supply chains: A grey relational analysis approach. *Journal of Cleaner Production, 86*(1), 343–359.
Ratick, S., Meacham, B., & Aoyama, Y. (2008). Locating backup facilities to enhance supply chain disaster resilience. *Growth and Change, 39*(4), 642–666.
Rice, J. B., & Caniato, F. (2003). Building a secure and resilient supply network. *Supply Chain Management Review, 7*(5), 22–30.
Scholten, K., Sharkey, S. P., & Fynes, B. (2014). Mitigation processes—Antecedents for building supply chain resilience. *Supply Chain Management: An International Journal, 19*(2), 211–228.
Schmitt, A. J., & Singh, M. (2012). A quantitative analysis of disruption risk in a multiechelon supply chain. *International Journal of Production Economics, 139*(1), 22–32.
Serdar-Asan, S. (2013). A review of supply chain complexity drivers. *Computers & Industrial Engineering, 66*(3), 533–540.
Sheffi, Y. (2004). Demand variability and supply chain flexibility. In G. Prockl, A. Bauer, A. Pflaum, & U. Müller-Steinfahrt (Eds.), *Entwicklungspfade und Meilensteine moderner Logistik* (pp. 85–117). Wiesbaden: Gabler Verlag.
Skipper, J. B., & Hanna, J. B. (2009). Minimizing supply chain disruption risk through enhanced flexibility. *International Journal of Physical Distribution & Logistics Management, 39*(5), 404–427.
Snell, P. (2010). Beware of the risks, and snap up the opportunities in 2010. In *IFPSM ezine Highlights.* Retrieved from http://www.ifpsm-ezine.org/S.
Soni, U., Jain, V., & Kumar, S. (2014). Measuring supply chain resilience using a deterministic modeling approach. *Computers & Industrial Engineering, 74*(2014), 11–25.
Spiegler, V., Naim, M., & Wikner, J. (2012). A control engineering approach to the assessment of supply chain resilience. *International Journal of Production Research, 50*(21), 6162–6187.
Swafford, P., Ghosh, S., & Murthy, N. (2006). The antecedents of supply chain agility of a firm: Scale development and model testing. *Journal of Operations Management, 24*(2), 170–188.
Tang, C., & Tomlin, B. (2008). The power of flexibility for mitigating supply chain risks. *International Journal of Production Economics, 116*(1), 12–27.

Thonemann, U. W., & Klein, M. (2011). Benefits of multi-stage inventory planning in process industries. *28. Deutscher Logistik Kongress*, 19.–21. October, Berlin.

Tomlin, B., & Synder, L. (2008). *On the value of a threat advisory system for managing,* s.l.: s.n.

Wieland, A., & Wallenburg, C. M. (2013). The influence of relational competencies on supply chain resilience: A relational view. *International Journal of Physical Distribution & Logistics Management, 43*(4), 300–320.

Zsidisin, G. A. (2003). Managerial perceptions of supply risk. *The Journal of Supply Chain Management, 39*(1), 14–26.

Part II
Creating Resiliency by Managing Supply Chain Risk

Chapter 6
What Value for Whom in Risk Management?—A Multi-value Perspective on Risk Management in an Engineering Project Supply Chain

Pelle Willumsen, Josef Oehmen, Monica Rossi and Torgeir Welo

1 Introduction: Value for Whom?

Imagine a simple scenario: You are on the verge of launching your new big project and the release date is also set. Failing to meet the launch date could be an extinction level event for your company. At the same time, your supplier is walking a financial tightrope and needs to keep the cost target, even if this will introduce delay in the project. There may be asymmetry in the value perceptions of the customer/OEM and the supplier regarding what value risk management should protect. The risk management performed by these stakeholders may serve to protect their own interests, but as a result jeopardize the project for both parties. In the following, we stress the importance of taking multiple stakeholder perspectives into consideration when designing supply-chain risk management systems.

Risk management (RM) results are used for decision-making and should provide value for decision-making stakeholders. However, determining what exactly this value is for each stakeholder is not typically covered in standard risk management practices. Our empirical studies (Sect. 3) showed that stakeholders have different views on what value risk management should or could provide to them as seen in Fig. 1; for example, the focus could be on keeping the cost of a project down or facilitating a clearer understanding of the requirements for a project or exploring the (feasible) solution space.

P. Willumsen (✉) · J. Oehmen
Technical University of Denmark (DTU), Kongens Lyngby, Denmark
e-mail: pwil@dtu.dk

M. Rossi
Politecnico di Milano, Milan, Italy

T. Welo
Norwegian University of Science and Technology (NTNU), Trondheim, Norway

G. A. Zsidisin and M. Henke (eds.), *Revisiting Supply Chain Risk*, Springer Series in Supply Chain Management 7, https://doi.org/10.1007/978-3-030-03813-7_6

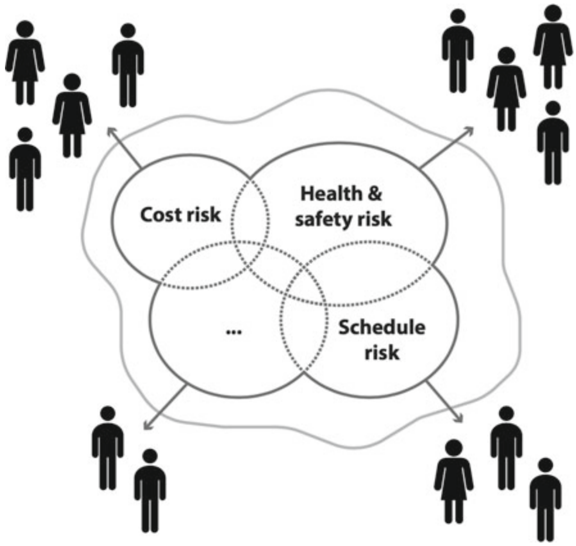


Fig. 1 Multiple value perspectives in supply-chain risk management

As context and stakeholders change between engineer-to-order (ETO) projects, supply chain and risk management teams need to determine on a project-by-project basis what value risk management should provide, and for whom.

2 Why Do We Need a Multi-value Perspective? Insights from Literature

If risk management (RM) is implemented as a standardized or highly formalized, compliance-driven activity, it can end up disconnected from the actual value creation and value perspectives of the relevant stakeholders (Kutsch et al. 2014; Lehtiranta 2014; Olechowski 2012). There is growing evidence that risk management is often ineffective. This is because RM does not work simply by identifying and managing risks with the help of methods and tools only; instead, it needs to be supported by certain critical success factors, including the integration of stakeholders into RM activities (Kutsch et al. 2014; Lehtiranta 2014; Oehmen et al. 2014).

There is a need for tailoring RM to stakeholder value perceptions and contexts (Petetin et al. 2011; Škec et al. 2014; Vasconcellos et al. 2011; Willumsen et al. 2018)—as opposed to doing business as usual—which in many cases refers to bringing out a required, standardized, compliance-driven risk management checklist. One of the paradoxes that exist in the SCRM of ETO projects is the competing need for standardization of risk management versus the need for tailoring risk management to stakeholders, unique situations and contexts (Cagliano et al. 2015; Chopra and Sodhi 2004). Tailoring or customization of the risk management activities and systems is needed (ISO 2009; Škec et al. 2014; Waters 2009; Willumsen et al. 2017), because of the needs of the stakeholders in relation to SCRM. The need for customization is also identified by ISO31000:2009. During the design of the risk management process, decisions need to be made on how to configure the RM process with appropriate methods and determine how these best fit together in a particular context (ISO 2009) to design a value-adding RM. Moreover, risk management should add and protect value (ISO 2009), but the question remains: *What is this value, and to whom?*

2.1 Supply-Chain Risk Management Perspectives and Perceptions

Supply-chain risk management (SCRM) should protect the interests of stakeholders, but stakeholder interests can be shared, neutral or conflicting, and SCRM is a "balancing act" (Waters 2009).

Zsidisin (2003a) identified a need for research on managerial perceptions of risk from different perspectives, and one study identified vast differences in what risk characteristics were perceived as significant by different stakeholders and that stakeholder perceptions of risks vary (Zsidisin 2003a). Risk is a multidimensional construct that often differs according to business function (Zsidisin 2003b). A resulting challenge for SCRM is how to consider these multiple perspectives.

Stakeholders can have different "risk profiles" and different perspectives on what risks are important (Hallikas 2009) and how risk management adds value. Gaudenzi (2009) links stakeholder perspectives and the achievement of overall objectives:

> The differing perspectives of the various actors involved should be carefully considered by the managers to prevent different companies or decision-makers from evaluating and assessing risks in different ways, since this might negatively affect the achievement of overall objectives. (Gaudenzi 2009).

Waters (2009) illustrates the potential of conflict between perspectives: One stakeholder perceives keeping stock low to reduce risk to profit, while another perceives keeping stock high to reduce the risk of disruptions. This also applies to our findings where stakeholders perceive risks and what impact on objectives is important to reduce very differently.

Agency theory suggests that a stakeholder may prioritize their own interests when given the responsibility for other opposing interests. The construction industry is known for stakeholders "adversarial" attitude towards each other (Ritchie et al. 2007), which was confirmed during our own empirical studies. Interviewees described that some contractors would try to withhold information about risks to capitalize on them later, highlighting the need to understand possibly conflicting interests that may show up in the SCRM (interviews, risk manager and project manager). It is problematic if one stakeholder focuses only on their "own" risks, because many risks in supply chains are often shared and networked across organizations. Organizations should therefore expand beyond their own interests when doing SCRM (Waters 2009) but a best practice gap exists for analysing risks in SCRM projects and processes utilizing a systemic perspective (Gaudenzi 2009).

Part of this systemic perspective is understanding stakeholders in RM. Specifically, who are the most important stakeholders and what are the value propositions or utility of SCRM for these stakeholders, both inside and outside the company?

2.2 Value for Stakeholders in Risk Management

To understand the value of risk management, we briefly consider characteristics and definitions of value, to use it as a frame of reference for understanding what value means in a risk management context.

The Cambridge dictionary defines value as the importance or worth of something for someone (Cambridge Dictionary 2016). Slack (1999) expands on this definition: "Value is a measurement of the worth of a specific product or service by a customer".

From these definitions, we can deduce important aspects to consider about risk management, such as its "worth" in decision-making. However, it is possible to extend the concept of value further:

Ouden (2012) expands the definition of value to include multiple stakeholders and describes value as being about meeting a need or objective of a stakeholder, including those which are explicit, implicit, unmet or perceived. Stakeholders exist on multiple levels such as a "user", an organization, an ecosystem or society, and value can be of many different types such as economic, social, environmental. The value of a certain type is different for a user and for an ecosystem and thus may differ at different abstraction levels (Gallarza and Gil 2006; Ouden 2012). When applied to risk management we find that dealing with some risks at the project level may not be value adding for the project team but may represent huge value for the organizational level.

We can expand the definition of value in multiple directions (Welo and Ringen 2016) and value can be very different from the perspectives of different stakeholders and in different contexts (Ouden 2012). The main insight to apply to risk management is that the value perception of project objectives can vary greatly between stakeholders, contexts and projects (Thomas 2008; Zhai 2009).

We link risk management and the value perspective based on the definition of a risk as "the effect of uncertainty on objectives" (ISO 2009). For the purpose of this paper, we equate "value" with "objective": Risk management is "valuable" to a stakeholder if it manages the effect of uncertainty on a specific value of this stakeholder.

The value perspectives found in our empirical studies (Sect. 3) span very broadly from tangible values, such as keeping the cost of a project down, to intangible ones, such as facilitating a clearer understanding of the requirements for a project and exploring the (feasible) solution space.

We have performed interviews to elicit the value perspectives of the contribution of risk management to ETO project success.

3 Empirical Study: The Multiple Value Perspectives of Risk Management for Stakeholders

Literature highlights the importance of considering stakeholders in risk management, however, there is a lack of empirical examples of stakeholder value perceptions of risk management. Starting from this gap, as a contribution to knowledge and practice, we conducted empirical research to explore the variety of perspectives on the value of risk management in industrial applications. This section first introduces the scientific research method that we followed to gather in-depth knowledge from the field and secondly to discuss the findings.

3.1 Research Method

To address the open issues in the literature and to derive practical implications on how to manage multiple value perspectives of RM among stakeholders, we performed an in-depth analysis in the industrial field. We focused on a sector which is mature in conducting RM initiatives and is complex enough to gather the challenges of different stakeholders' perspectives: the construction industry. Specifically, we studied three companies operating in large-scale engineering projects in the construction sector. We elicited 30 semi-structured interviews (Blessing and Chakrabarti 2009) with project practitioners involved in project risk management at different hierarchical levels and roles as seen in Table 1. Part of the semi-structured interview design was based on the hypothesis that it is beneficial to consider stakeholder value perspectives in the design of RM (Willumsen et al. 2017). In addition to the semi-structured interviews, we performed contextual analyses of RM boundary objects within the companies. This included, but was not limited to, risk management systems for reporting risk, central risk management reporting structures, workshop documentation and training, risk matrices, risk registers, risk logs, reporting systems for steering group communication. Additionally, we observed risk workshops performed within and by each company and did semi-structured follow-up interviews.

To validate and expand the findings, we conducted three practitioner workshops with over 100 participants. While one workshop involved only practitioners from the construction industry, the other two involved participants with different backgrounds, from both the construction industry and other industries with the aim of validating and generalizing the achieved results beyond the construction industry.

Table 1 details the 30 interviews that were performed, as well as all the other analyses that were conducted, i.e. four observations, analysis of four RM artefacts (see Table 1) and 3 workshops. The interview group consisted of PMO, CEO, CFO, project controls, RM specialists and project portfolio managers in the investigated companies acting as either client, supplier or both (Table 1).

Table 1 Overview of the empirical data collection, interviews and observations

Interviews						
Company 1	PMO	Portfolio management	Project management	Internal RM consultant	Project risk management team lead	Project controls
Company 2	RM specialists	Client advisors	(CEO)	Project management		
(Company 3)	CFO	PMO	(CEO)			
Observations						
Company 1	Monthly meeting	Quarterly meeting	RM workshop	RM system	RM documentation	
Company 2					RM documentation	
Company 3					RM documentation	

We created affinity diagrams using a grounded theory approach (Beyer and Holtzblatt 1998) and coded the interviews in value propositions with a team of risk management and project management experts to identify key constructs in an iterative process. Through this approach, we identified and structured the value propositions gathered from both empirical studies and literature. The study was carried out over the course of 1 year with multiple follow-up interviews. Our findings show a wide range of primary values associated with risk management, spanning both project context and project level execution. The following introduces the reader to these findings and elaborates on the concept of multiple value perception in RM when different stakeholders are involved.

3.2 *The Multiple Value Perspectives of Risk Management for Stakeholders*

The aim of the empirical analysis was to identify if and to which extent multiple stakeholders share the same value propositions in SCRM. Results show that the concept of the value of risk management significantly changes between stakeholder groups. To quote statements made by interview participants directly, different values include "keep the project on target", "support decision-making", "assist the prioritization of efforts", "help to avoid deaths", or "assist exploration of the solution space". Logically, different perceptions of value can lead to conflicts when it comes to defining what value risk management is supposed to provide.

These differing perceptions affect everything from how stakeholders evaluate risks for the project, to how the process is carried out. For example, from the interviews, workshop material and risk logs it was found that customers/OEM and suppliers have different perceptions of what the important risks are. Even within customers' and suppliers' organizations, there are differing and opposing perceptions depending on business function and hierarchy level, about what important risks are and about how the process should be carried out, and why.

The value of risk management is related to what objectives it may serve to protect. Indeed, even though the people interviewed share the concept that risk management provides value by helping to prioritize tasks in terms of risks to the objective, the main differences were found in terms of what objective was in focus; this clearly differed depending on the roles of the interviewees and the RM objects being studied. For instance, while upper management was focused on risk at strategic level (e.g. what was the market context of the project), project managers focused on risk at operative project level. The different perceptions ultimately affect what value (objectives and impact) is in focus and how SCRM is carried out (process quality). Indeed, results from empirical research show heterogeneity here, but suggest that the main differences in value perspectives among multiple stakeholders occur in terms of the outcome and the process quality of risk management—the value of the process of RM itself. The outcome dimensions include straightforward goal conflicts between stakeholder perceptions; however, a more complex story emerges around what constitutes a good process for a stakeholder. The following paragraphs address these points.

3.3 The Outcome-Related Value Perspective of Risk Management

3.3.1 Value Perspectives of Risk Management: Project Level

Multiple interviewees, i.e. project managers, a risk manager and a portfolio manager, described the key value of SCRM at the project level as "keeping the project on target", a proxy for achieving project success. The most frequently mentioned targets were cost and schedule. However, the target that was being referred to differed between the stakeholders. For example, in one case a first-tier supplier focused on quality and cost while the client focused on schedule, creating a tension in the way risks were managed. Eight value dimensions were identified at the project level: Schedule, cost, quality, scope, health and safety, environment, technical feasibility and customer satisfaction.

In the case studies carried out in company 1, a development department represented a supplier relationship internally. Their output was key for a much larger department's projects, and therefore, some degree of cost overrun was not important. Rather than cost, the main values that risk management provided for this department were to help keep the project on schedule. The RM was designed towards risk to schedule as the primary value dimension of importance for this internal stakeholder.

Table 2 Example of possibly conflicting and shared value dimensions of risk management

	Value dimensions		
	Quality	Cost	Customer satisfaction
Stakeholder 1	X		X
Stakeholder 2		X	X

X: Shared value

X: Possible conflict (or indifference)

"We express [risk] impact in terms of how it affects schedule", (project manager in the development department).

In the case study of company 2, a client advisor overseeing a large portfolio of projects within the construction industry described that the target focus can change from client to client. With a public works client, the main value of risk management was to keep the project on cost as the main target, but for a large private engineering client it was reputation, schedule and quality. In the examples described, the function of the RM was to assist in keeping the project on target, but this target varied between stakeholders, even on the same project, between the client and suppliers.

The value of risk management was found to differ across company functions. Through interviews and by observing RM objects, a tendency was identified that the finance department focuses on "keeping the project on cost" while R&D focused on "technical feasibility" and management focused on "being on schedule and cost". These different focuses on what it means to keep a project on target was found to be a conflict of interest, have no relation or a shared value driver (as seen in Table 2) with regard to the risk management and how it was performed.

The dimensions that define the ETO project success drive the focus and value of risk management, and if stakeholders have conflicting perspectives on the success of the project it shows up in the way they perform risk management.

3.3.2 Value Perspectives of Risk Management: Strategy/Project Context Level

It was observed through interviews and study of RM logs that the value of risk management at the strategic—or project context—level related to other value dimensions than at the project level. Value dimensions such as "reputation/brand" or "market share" may supersede "cost" on the project level and some cost overrun may be accepted so as to achieve a higher goal for the company. One interviewee stated that project managers sometimes overlook the "bigger picture" when they manage risk

Table 3 Overview of outcome-related value dimensions

	Value dimensions							
Project level	Cost	Quality	Schedule	Scope	Health & Safety	Environment	Customer satisfaction	Technical feasibility
Project context/ strategic level	Growth	Market share	Profitability	Innovation	Cash flow	Reputation/ brand	Culture	Compliance

and opportunities in their project. For example, cost overrun on a project may be acceptable (or negligible), if the project is a vehicle for a strategic objective. Management opportunities can be overlooked when teams only consider risk to their own "backyard". It was observed in an RM workshop in company 1 and revealed in interviews with upper management and senior project managers in company 1 and 2 that their project managers sometimes do not prioritize the "higher level" objectives of their project risk management.

RM addresses eight value dimensions at the project context level: Growth, market share, profitability, cash flow, innovation, reputation, culture and compliance.

Conflicts may occur between the project value dimensions but also between project and project context level. The value dimensions identified on both levels are shown in Table 3.

3.4 The Process Quality-Related Value Perspectives of Risk Management

Several value dimensions emerged from the empirical investigation addressing the quality of the SCRM process itself and its contribution to the overall SCM and ETO project management process quality. They are creating transparency regarding risk exposure, improving forecasting quality, facilitating high-quality requirements, exploring the feasibility of the solution space, enabling employees to speak up and supporting decision-making—The go/no-go decisions (Table 4). Each of them is briefly introduced in the following section.

Table 4 Overview of the process quality-related value dimensions of risk management

	Value dimensions					
Process quality level	Transparency regarding risk exposure	Improving forecasting quality	Facilitate high quality requirements	Exploring the feasibility of the solution space	Enabling employees to speak up	Supporting decision making: go/no-go decisions

3.4.1 Transparency Regarding Risk Exposure

The empirical findings as well as empirical studies in the literature (Oehmen et al. 2014) identify transparency regarding risk exposure as a very important aspect of good RM. Transparency is a key factor affecting proper risk-informed decision-making at any given time. The perspective of upper management in the interviews was that of creating transparency regarding risk exposure, the “right” stakeholder can make the “right” decision. This perspective was also evident in the set-up of risk management tools and reporting system set-up.

However, creating transparency through risk management has conflicting value for some stakeholders. Interviews revealed that at times, suppliers might not share knowledge about certain risk exposure, to then capitalize on it later.

Transparency can be a dual-edged sword according to multiple interviewees, and it is quite common for project managers to “do their own thing [risk management] on the side”, which refers to having an “offline” risk management system not visible to anyone outside the project. In the process of communicating risks to top management, project managers may leave out certain risks that would for instance put their own project at risk of being cancelled or have other consequences for them. It was identified by interviewees that often PM’s wait too long to escalate a risk thereby creating a situation where PM does not receive help in good time and the top management’s ability to make decisions is hindered.

Multiple companies in the study presented examples of how transparency regarding risk exposure is perceived differently, as described in the following. In the early phases, RM results were used as a way to “sell” the project and the focus was on making the project feasible rather than identifying all risks. In this context, RM was providing value for the sales personnel showing an “acceptable projects risk profile” through underestimation of the risks. This is identified as a common industry phenomenon and could be because it may not be possible to get the green light for a project, if the risk management paints a too “gloomy picture”. In sensitive situations, the focus is on getting the project approved. Risk assessments were perceived as enablers in that situation, that can help to get a project approved or not approved depending on how risky a project is perceived to be. The value that sales perceive risk management to have is in conflict with what a PM needs, which is a conservative risk estimate as seen in Fig. 2.

Fig. 2 Conflicting perspectives in risk management

3.4.2 Assisting the Prioritization of Efforts

According to interviewees and our study of risk management reporting systems and risk logs, RM provides different value for different stakeholders in relation to prioritizing efforts on the strategic and project level. If a project manager identifies an important risk during a risk management activity, he will choose to perform an action in relation to this risk. The same was found to be the case for upper management; however, it was only larger risks that were used for prioritizing efforts. From this we find that RM is used to prioritize work tasks at the project level and resources and strategic direction on the upper management levels, as seen in Fig. 3. The value of RM was described as to be a forward-looking "radar" that identifies incoming threats before they materialize by creating awareness and enabling stakeholders to prioritize efforts in relation to them.

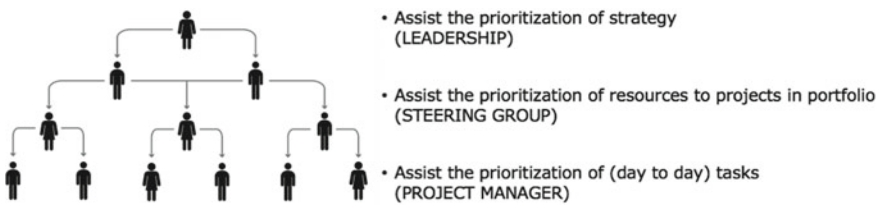


Fig. 3 Different value perceptions of risk management at different levels in a company

3.4.3 Improving Forecasting Quality

"Sometimes they just rub the crystal ball". A risk specialist described the value of SCRM as a way to increase the quality of forecasts by incorporating risk management results in them, instead of solely relying on the aforementioned crystal ball. It was observed and stated that forecasts during projects are often based on a lacking indicators, such as invoices, which, in the experience of the interviewees, are inherently uncertain as we cannot necessarily predict the future from historical data. The value of RM in this context was discovered to be twofold by risk management experts working at the portfolio level: To increase the understanding of the quality of forecasting through adding data, increasing the quality of data, as well as revealing assumptions in the data. Workshops and interviews revealed that at the leadership level or CxO level, this equates to "better business predictability" but at the PM level it is sometimes a sham exercise carried out to satisfy compliance. In this example, understanding the actual process quality value perception for stakeholders becomes crucial.

3.4.4 Facilitate High-Quality Requirements

Better understanding of requirements is a key need for all stakeholders involved. Through interviews and by studying RM boundary objects and reporting, risk management can be intimately tied to requirements. Examples include a client advisor and management who used the RM framework to have conversations about the quality of the requirements. They used the RM artefacts to ask "did we understand the requirements correctly" to try to facilitate an improved understanding of the uncertainty in the requirements that had been originally recorded. Changing orders late in the process in the construction industry was identified as a major risk, and this was believed to be tied to the quality of the requirements such as miss-alignments in the understanding of these by different stakeholders. Several of the interviewees pointed out that risk management process quality plays a direct or indirect role in relation to requirements quality.

One conflict that may arise in relation to requirements, as reported by a client advisor, a PM and an RM expert, is that a supplier might withhold information about risks related to requirements. The supplier then later uses this information to capitalize on risks while the client advisor or PM will try to "put all the risks on the table" up front so as to make a proper estimate. The interviewees explained that it is in the best interests of the client to know the risks up front too, but not in the interests of the suppliers, as it represents an upfront investment for them to reveal everything, and in some cases, these risks form part of their profitability.

3.4.5 Exploring the Feasibility of the Solution Space

Solution space can be defined as the overall set of possible solutions that could be applied to a system/sub-system to accomplish requirements, and functionalities which the system/sub-system is supposed to include. The challenge for stakeholders is to figure out if a solution, even though it might seem enticing at first, is actually part of the solution space or not. Empirical observations suggest that RM plays a role in this because it is responsible for the risk profile of that particular solution in relation to the project and stakeholders. A client advisor, portfolio manager in R&D and a risk manager all operating in the construction industry, noted that RM assists the exploration of the solution space as it can determine if a solution is too risky in relation to a type of potential impact on the project. This could occur in terms of "innovation" or newness of the concept or potential cost or something else. Risk management reveals that feasibility is highly context-dependent and helps to reveal if a part of the solution space is relevant or not. A development team and portfolio manager identified RM as a way to understand if a solution would be feasible. This included how it would affect stakeholders, such as customers and existing production, ultimately placing RM as central to feasibility.

A risk manager and supplier expressed that clients and architects "just want to design" without prioritizing feasibility, and a client presented the counter-argument that "the engineers just want to make it standard and ugly".

A portfolio manager explained that RM at stage gate review helped identify big potential problems within a project with regard to safety and the public perception that the engineers had not understood because they had focused mainly on the technical feasibility.

3.4.6 Enabling Employees to Speak Up

The SCRM was described multiple times as a critical way for engineers or project managers to reach out to the leadership about serious risks, the need for resources, or about risks going beyond the scope of the project. In some instances, SCRM is a way for the project team "to be heard".

Risk management is of value to the project when it comes to risks that cannot be handled by the project, and it is a communication channel for the company, according to workshop participants and project controls as employees are often closest to the information about risks that are needed by upper levels in the organization. Company attitudes towards rewarding "firefighting" or reactive problem-solving as a cultural approach result in conflicts with employees speaking up proactively on risks, which can create a counterproductive environment for identifying risks.

3.4.7 Supporting Decision-Making: The Go/No-Go Decisions

Multiple interviewees mentioned that steering groups, portfolio managers and leadership use high-level RM results for evaluating if a project should continue or not. The upper level of management has a need to understand the risk profile of a project or portfolio to determine the right course of action in relation to the company goals and strategy. In one of the cases, interviewees described engineers presenting a concept where they focused primarily on technical risks, but excluded health and safety, even though this was crucial for the company. The risk management provided value by identifying these other perspectives and the tension between them. Multiple interviewees stated that risk management results were used in decision-making and that supporting decision-making is a central value that risk management provides, but conflicts occur between different functions of the company and between project and strategic level.

3.5 Discussion: Learnings from Empirical Studies

The findings and discussion presented above show that there are significant differences between stakeholders and their perceptions of value, through both literature and empirical studies. An important finding is based on the fact that if those perceptions remain unaligned, they can significantly impact the quality of the SCRM process. To address this issue, the following section proposes a method to be used to support an alignment process in SCRM.

In one of the cases studied, the RM was customized to record and utilize value perceptions on risk from different stakeholders so as to improve decision-making through transparency. In another case which was studied, a framework was developed to ensure the awareness of multiple stakeholder perspectives on risk.

Research shows a tendency that stakeholders can have different "value profiles", e.g. specific and reoccurring outcomes and process qualities they prioritize and value. It is potentially very problematic if stakeholder perceptions are not considered in the SCRM, including potential conflicts—as is evident in the literature as well as in the empirical work presented here. With knowledge about stakeholder value perspectives and potential conflicts, improvements to the design of the SCRM can be identified and carried out, as discussed in the following.

3.6 Process Regarding Multi-value Perspectives

Empirical work and the preliminary validation of the above-mentioned practitioners' workshops enabled the introduction of a process able to incorporate a multi-value perspective in SCRM (see Fig. 4), through the formal steps of (i) sensitizing a team to multi-value perspectives; (ii) exploring the stakeholder landscape; (iii) eliciting

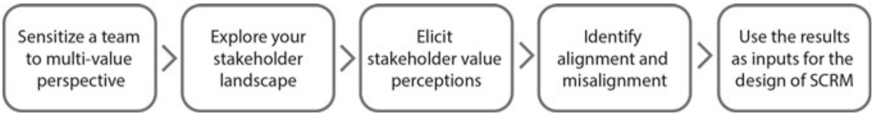


Fig. 4 Process for establishing a multi-value perspective in supply-chain risk management

stakeholder value perceptions; (iv) identifying alignment and misalignment; and (v) using the outcome as input for SCRM design. Each step is described in the following.

Sensitizing a team to a multi-value perspective The examples and concepts in this chapter can be used to sensitize a team to the competing, yet valid value perceptions that exist for SCRM. Alternatively, it can be achieved by creating a vicarious experience of viewing risk management from different stakeholder perspectives. Taking on the vantage point of different stakeholders will help a team to recognize the variations in value perspectives. Different stakeholders have different perspectives. Awareness of these perspectives can enable a team to take them into account to foster collective and systems-oriented thinking as well as to bridge company silos.

Explore your stakeholder landscape Explore the stakeholder landscape and the different values risk management can provide for it as a system. This can be achieved through established stakeholder management techniques such as stakeholder maps.

Elicit stakeholder value perceptions Elicit stakeholder value perceptions of risk management regarding outcomes and process quality utilizing Table 5 as a template or preliminary checklist of value perceptions.

To understand a stakeholder's value perception of risk management, value dimensions of importance for stakeholders must be considered—*What do they value most?*

Table 5 Overview of value dimensions. The overview can be used for eliciting value perspectives regarding risk management

		Value dimensions							
Project Outcome	Project level	Cost	Quality	Schedule	Scope	Health & Safety	Environment	Customer satisfaction	Technical feasibility
	Project context/ strategic level	Growth	Market share	Profitability	Innovation	Cash flow	Reputation/ brand	Culture	Compliance
Process quality level		Transparency regarding risk exposure	Improving forecasting quality	Facilitate high quality requirements	Exploring the feasibility of the solution space	Enabling employees to speak up	Supporting decision making: go/ no-go decisions		

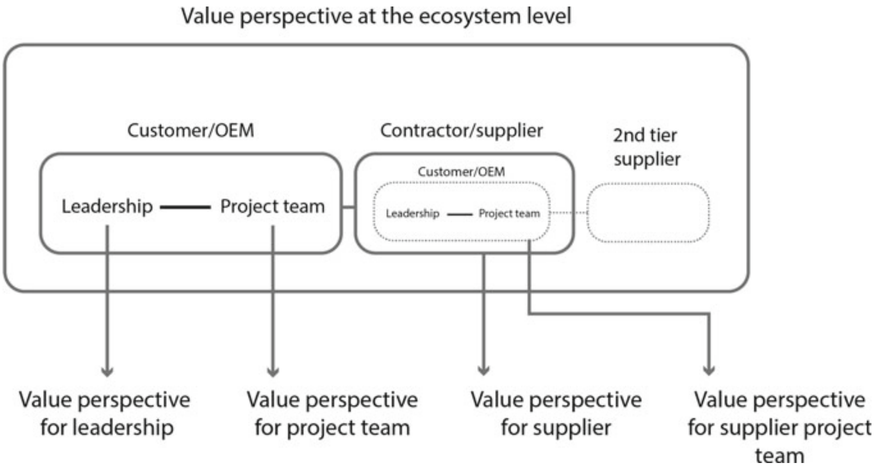


Fig. 5 Value propositions of risk management exist at different levels inside and outside the companies, as well as at the ecosystem level

The elicitation of value perspectives should include different levels within and outside the companies, as well as the system or "ecosystem" level in both the two dimensions of project outcome (either project level or strategy/project context level) and quality process level. As depicted in Fig. 5, various stakeholders have different value perspectives of risk management inside and outside the company and at the ecosystem level.

Identify alignment and misalignment Using the knowledge about the stakeholder landscape and the value perspectives of the stakeholders from the previous steps, we can identify and reflect about the alignment or misalignment of value perceptions of SCRM across the stakeholder landscape using a matrix of stakeholders and value perceptions as illustrated in Tables 6 and 7. The tables can help with a systematic and visual approach to assessing stakeholder conflicts and shared value perceptions of risk management.

All levels should be checked for conflicts and shared values in the models presented, as depicted in Tables 6 and 7. The tables add an overview and assist in identifying possible conflicting value perceptions that affect the RM. Specifically, RM should address these potential conflicts to optimize how risk is managed at the individual and systems level. If we do not consider the multi-value perspective on RM, we run the risk of adversarial dynamics and missed opportunities for leveraging shared drivers in the design of the RM.

Table 6 Illustrative example of alignment and misalignment of stakeholder value perceptions of risk management

Alignment: Shared and conflicting value perceptions of risk management				
	Customer/OEM-Leadership	Customer/OEM - Project team	Supplier-Leadership	Supplier-Project team
Customer/OEM-Leadership				
Customer/OEM - Project team	Conflicting value proposition; Transparency			Conflicting value proposition: Schedule vs. cost
Supplier-Leadership	Shared value proposition: Transparency regarding risk exposure	Conflicting value propositions: Cost vs. quality		
Supplier-Project team				

Table 7 Illustrative example of alignment and misalignment of value perceptions of risk management

Value dimensions

	Quality	Cost	Customer satisfaction
Stakeholder 1	X		X
Stakeholder 2		X	X

X: Shared value
X: Possible conflict (or indifference)

Tables 6, 7 and 8 serve as illustrative examples of alignment matrices that may be used as a visual support for designing the SCRM based on information from the previous steps.

Table 8 Illustrative example of an alignment matrix with shared and possibly conflicting value perspectives of risk management

Alignment: Shared and conflicting value perceptions of risk management				
Project level	Customer/OEM - Leadership	Customer/OEM - Project team	Supplier - Leadership	Supplier - Project team
Cost		x	x	x
Schedule	x	x		x
Quality	x	-		
Customer satisfaction	x	x	x	x
Project context level				
Reputation	x		x	
Profitability	x		x	
Market share				
Process quality level				
Transparency	x	-	-	-
Enable employees to speak up		x		
Requirement quality		x		

Shared ———
Possibly conflicting or indifferent - - - - -

Use the results as input for the design of SCRM The previous steps generate insight that is extremely useful for addressing the design and execution of SCRM. The awareness of potential conflicts and shared value perceptions can be leveraged to tailor the SCRM and chose appropriate approaches and structure of the SCRM. The value dimensions both related to outcomes and process quality can be used to elicit a stakeholder's value profile but also as inspiration for the potentially relevant value perspectives that are missing, and could potentially improve the SCRM.

4 Conclusions

This chapter addresses the issue of introducing RM initiatives appropriately along the supply chain by embracing a multi-stakeholder perspective. By discussing the experiences collected throughout this in-depth empirical research, and with the aim of overcoming the main drawbacks which exist in practice—and which have not yet been completely addressed by either academia or industry—we propose following a practical multi-step process in order to address the main criticalities related to stakeholder perceptions when defining a comprehensive and effective SCRM.

Two main important insights emerged from empirical evidence:

1. It is crucial to understand the value propositions of SCRM for different stakeholders at different levels inside and outside a company. Taking the stakeholder value propositions of SCRM into account when designing the SCRM is beneficial as it can enable the identification of conflicting value profiles and leverage shared ones.
2. SCRM should be tailored to be "fit for purpose", and the multi-value perspective is one aspect that is relevant for tailoring or customizing the SCRM.

The methodology presented here helps to elicit value propositions regarding risk management that can then be used to tailor or customize the SCRM.

Designing the SCRM according to multiple stakeholder value perspectives and contexts can enable a better fit with each project, making sure that SCRM becomes much more than a tick the box exercise. Like any system, the design of the system can benefit from revealing its stakeholders and the value the system potentially can provide for them. Taking the value into account does not mean always catering for a stakeholder's need, rather it means to cater to some and deal with some in other ways, but especially dealing with conflicting value propositions and leveraging shared ones. For instance, if a contractor tries to hide risks to capitalize on them later or if sales underestimate the risks, the designers of the SCRM can try to prevent it by design, for instance through creating additional transparency. The value that SCRM needs to protect and provide has to be customized to each project to some degree, because different stakeholders have different priorities, such as was the case with the client who focused on schedule and quality, and another client who focused on cost.

A contextual approach to the design of SCRM should be followed. Even though many authors advocate taking stakeholder interests into account, here we have presented an in-depth account of what that means based on empirical studies as well as on a hands-on methodology. The value propositions presented here can also be used as a "checklist" to help when having conversations with relevant stakeholders and to gain insights which can be used in the design of SCRM and to discover areas for improvement that have potentially been overlooked.

References

Beyer, H., & Holtzblatt, K. (1998). *Contextual design: Defining customer-centered systems*. Burlington, Massachusetts: Morgan Kaufmann.

Blessing, L. T. M., & Chakrabarti, A. (2009). *DRM, a design research methodology*. London: Springer. https://doi.org/10.1007/978-1-84882-587-1.

Cagliano, A. C., Grimaldi, S., & Rafele, C. (2015). Choosing project risk management techniques. A theoretical framework. *Journal of Risk Research*, *18*(2), 232–248. https://doi.org/10.1080/13669877.2014.896398.

Cambridge Dictionary, C. (2016). Cambridge dictionary. *Meaning*, (entry 124), 138–138.

Chopra, S., & Sodhi, M. S. (2004). Managing risk to avoid supply-chain breakdown. *MIT Sloan Management Review, 46,* 53–61. https://doi.org/10.1108/IJOPM-10-2012-0449.

Gallarza, M. G., & Gil, I. (2006). Value dimensions, perceived value, satisfaction and loyalty : An investigation of university students' travel behaviour. *27*, 437–452. https://doi.org/10.1016/j.tourman.2004.12.002.

Gaudenzi, B. (2009). Assessing risks in projects and processes. *International Series in Operations Research and Management Science*, *124*.

Hallikas, J. (2009). Risk management in value networks. *International Series in Operations Research and Management Science*, *124*.

ISO. (2009). ISO 31000:2009 Risk management—Principles and guidelines. Retrieved from http://www.iso.org/iso/home/standards/iso31000.htm.

Kutsch, E., Browning, T. R., & Hall, M. (2014). Bridging the risk gap: The failure of risk management in information systems projects. *Research Technology Management, 57*(2), 26–32. https://doi.org/10.5437/08956308X5702133.

Lehtiranta, L. (2014). Risk perceptions and approaches in multi-organizations: A research review 2000–2012. *International Journal of Project Management, 32*(4), 640–653. https://doi.org/10.1016/j.ijproman.2013.09.002.

Oehmen, J., Olechowski, A., Robert Kenley, C., & Ben-Daya, M. (2014). Analysis of the effect of risk management practices on the performance of new product development programs. *Technovation, 34*(8), 441–453. https://doi.org/10.1016/j.technovation.2013.12.005.

Olechowski, A. (2012). Characteristics of successful risk management in product design. In *Proceedings of International Design Conference, Design*, *DS 70*.

den Ouden, E. (2012). *Innovation design: Creating value for People*. Organizations and Society: Springer. https://doi.org/10.1007/978-1-4471-2268-5.

Petetin, F., Bertoluci, G., & Bocquet, J. C. (2011). Decision-making in disruptive innovation projects: A value approach. In *International Conference on Engineering Design (August)*.

Ritchie, B., Brindley, C., & Brindley, C. (2007). Supply chain risk management and performance. *International Journal of Operations & Production Management, 27*(3), 303–322. https://doi.org/10.1108/01443570710725563.

Škec, S., Štorga, M., Rohde, D., & Marjanović, D. (2014). Tailoring risk management approach for the product development environment. In *Proceedings of the 13th International Design Conference (DESIGN 2014)* (pp. 385–396).

Slack, R. A. (1999). The lean value principle in military aerospace product development. *The Lean Aerospace Initiative*, *17*.

Thomas, J. (2008). Researching the value of project management. *PM Network, 22*(12), 79. https://doi.org/10.1002/pmj.20105.

Vasconcellos, V., Grubisic, F., & Gidel, T. (2011, August). Recommendations for risk identification method selection according to product design and project management maturity, product innovation degree and project. *Design*.

Waters, C. D. J. (2009). *Supply chain management: An introduction to logistics*. London: Palgrave Macmillan. Retrieved August 30, 2017, from http://findit.dtu.dk/en/catalog?utf8=✓&locale=en&search_field=all_fields&q=donald+waters+supply+chain.

Welo, T., & Ringen, G. (2016). Beyond waste elimination: Assessing lean practices in product development. *Procedia {CIRP}*, *50*, 179–185. http://dx.doi.org/10.1016/j.procir.2016.05.093.

Willumsen, P., Oehmen, J., Rossi, M., & Welo, T. (2017). Applying lean thinking to risk management in product development. In *Proceedings of the International Conference on Engineering Design, ICED* (Vol. 2).

Willumsen, P. L., Oehmen, J., & Ernstsen, S. K. (2018). Reconceptualizing design risk management as a learning strategy. *International Design Conference-Design, 2018, 5,* 2529–2540. https://doi.org/10.21278/idc.2018.0224.

Zhai, L. (2009). Understanding the value of project management from a stakeholder's perspective: Case study of mega-project management. *Project Management Journal—Project Management Institute*. https://doi.org/10.1002/pmj.

Zsidisin, G. A. (2003a, January). Managerial perceptions of supply risk. *The Journal of Supply Chain Management*, 14–26.

Zsidisin, G. A. (2003b). A grounded definition of supply risk. *Journal of Purchasing & Supply Management, 9,* 217–224. https://doi.org/10.1016/j.pursup.2003.07.002.

Chapter 7
Risk Management of Critical Logistical Infrastructures: Securing the Basis for Effective and Efficient Supply Chains

Michael Huth and Sascha Düerkop

1 Introduction

In summer 2017, parts of the railway network close to the German town of Rastatt sagged due to construction works for a new railway tunnel. Consequently, the route between Karlsruhe (Germany) and Basel (Switzerland) had to be fully closed for a duration of almost two months for both passenger and cargo transportation. The affected section of the railway network is a critical infrastructure for logistics: every day, approximately 200 cargo trains pass this link that connects Germany, the Netherlands, and Belgium with Switzerland and Italy. For those cargo shipments, the closure meant a severe problem. Some of the trains could be redirected, if bypasses were available and offered enough capacity; some trainloads could be transferred to road transportation or shipped on inland waterways. However, many shipments were put on hold and could not be delivered as planned. The activities to ease the problem led to an estimated additional cost for the railroad companies (excluding Deutsche Bahn) of almost 100 million EUR (Heinrici 2017). DB Cargo, a subsidiary of Deutsche Bahn, claimed lost revenues of another 46 million EUR (Schlesiger 2017).

This example shows that the logistical infrastructure plays a vital role in many developed countries for enabling both effective and efficient logistic chains. If one or more elements of the logistical infrastructure network are—even temporarily—not useable, logistic chains can be heavily affected. Thus, parts of the logistical infrastructure can be called critical.

M. Huth (✉) · S. Düerkop
Department of Business, Fulda University of Applied Sciences, Fulda, Germany
e-mail: michael.huth@w.hs-fulda.de

S. Düerkop
e-mail: sascha.dueerkop@w.hs-fulda.de

G. A. Zsidisin and M. Henke (eds.), *Revisiting Supply Chain Risk*, Springer Series in Supply Chain Management 7, https://doi.org/10.1007/978-3-030-03813-7_7

Possible events, that could lead to damages of the critical infrastructure (and consequently to additional cost) and threaten the economy of a county, will be stated as risks. Risk management, therefore, aims to identify, analyze, and evaluate risks as well as to develop and implement counteractive measures that should lead to a reduction of the probability of a risk and/or its consequences.

Risk management can be characterized by a closed loop of phases. The risk management loop can have the form of the iterative phase concept described in ISO 31,000. This article will focus on a specific step of the risk management loop: the risk evaluation. This phase aims to quantify previously identified risks so that they can be sorted by priority. Top priority risks are then managed immediately, whereas the management of low-priority risks might be postponed to a later stage. Thus, the risk evaluation leads to the recognition of the important and the less important risks.

In this article, we will develop an approach to how risks in logistical infrastructures can be evaluated. This should enable decision makers in risk management to make better (i.e., more justified) decisions and prioritize counteractions. We will start by giving examples for risks that can apply for critical logistical infrastructures following the PESTLE approach. We will then develop the evaluation approach, specify implementation aspects, and discuss its strengths and weaknesses as well as options to extend the approach. The chapter will be completed by a summary and an outlook on further research directions.

2 Risks for Critical Logistical Infrastructures

To ensure that all different fields of possible risks are thoroughly covered and systematically considered, a political, economical, social, technological, legal, and environmental (PESTLE) approach is used in the following. By investigating the keywords defined by the PESTLE abbreviation, it is ensured that no major possible risk factor is completely ignored or rejected. Albeit a completely qualitative approach, it serves as a capable method to give a first picture of the vast variety of risks the logistical infrastructure is typically exposed to.

Political risks are usually diversified into two separate sub-categories: macro-political and micro-political risks (Sottilotta 2013). While macro-political risks are not directly linked or directed to the affected business sector, namely the logistical infrastructure, micro-political risks are exactly that.

Macro-political risks, which can severely affect the logistical infrastructure, are all kinds of armed conflicts, including but not limited to full-scale wars, guerilla wars, and terrorism. In such volatile turmoil, infrastructural nodes and links, such as bridges, tunnels, train stations, or airports, are often either collateral damage or strategically targeted by bombing or other armed aggression. Recent examples include the Donetsk International Airport (Ukraine Today 2015), which has been defunct since mid-2014, the complete destruction of all bridges across the Euphrates River in the Syrian governorate of Deir ez-Zor (Zaman and Alwsl 2016), which were bombed by a US-led coalition air strike, or the Port of Aden, which was closed down for months during the years 2016 and 2017. Furthermore, terrorist attacks deliberately targeted populated parts of the logistical infrastructure to maximize the effect of their actions, as the terrorist attack in Brussels 2016 (McKenzie 2016), which affected the tram service and airport of the city, showed to devastating effect. Other forms of macro-political risks through terrorism include maritime terrorism, such as the piracy at the Horn of Africa, or a plotted terrorist attack of the Ohio trucker Iyman Faris, who planned to bring down Brooklyn Bridge (CNN 2003).

Micro-political risks do not necessarily coincide with aggression and include diplomatic meltdowns, which regularly lead to complete blockades and border closures. As such border closures affect the logistical infrastructures by cutting them, they can be seen as classic examples for micro-political risks. The most striking example for such a complete border closure is the border that separates the Korean Peninsula into the Democratic Republic of Korea and the Republic of Korea. As a result of the impenetrability of the border, the largest logistical infrastructure in history, the proposed 'Asian Highway 1 (AH1)' from Edirne (Turkey) to Tokyo (Japan), has never been passable from its start to its end. Other examples of complete border closure due to diplomatic meltdowns include the Armenian-Turkish land border, which has left the once crucial Kars (Turkey)–Gyumri (Armenia)–Tbilisi (Georgia) railway defunct since 1993 (Uysal 2014). In very rare occasions, even airports can suffer from micro-political risks, when the region the airport is located in is not internationally recognized (anymore). Currently, such theoretically operational, but de facto defunct airports can be found in the disputed territories of Palestine (Watson 2014), Cyprus (Morley 2013), and Nagorno-Karabakh (Asbarez 2016).

Economical risks are usually less relevant for the logistical infrastructure, as the majority of the infrastructure is typically publicly owned and thus well protected against bankruptcy. On the contrary, the few privately owned parts of the logistical infrastructure are often vulnerable to economical risks and can, in some cases, be critical for the overall infrastructures. Most prominently, airports are regularly vulnerable and highly critical simultaneously. The planned 'Berlin Brandenburg Airport', for instance, which should have replaced three smaller airports in Berlin by 2010, but is to date still not operational, caused an average monthly cost of well over 40 million Euro, due to necessary re-routings, re-licensing of the airports to be replaced and other infrastructural follow-up costs. The road infrastructure, which is often completely publicly owned, is also becoming more vulnerable to economic risks whenever public–private partnerships are realized. A warning example for this is the 'Camino Colombia Toll Road', which was built to connect Texas with Mexico, but went bankrupt and was completely closed after only four years of operation (US PIRG Education Fund 2009).

Social risks, by definition, affect individuals or groups of individuals who are then, after the realization of the risk, incapable of retaining their social status. Usually, individuals are not able to debilitate the logistical infrastructure in the following, but again several exceptions prove that social risks can, indirectly, affect logistical infrastructure severely. Most commonly, strikes by workers whose social status is at risk regularly affect the logistical infrastructure. In particular, airports and rail operations are repeatedly brought to a standstill by coordinated strikes. More drastically, a coordinated general strike directed against the oil supply chain caused a shortage of gas supplies for Greater Paris in 2016. During this orchestrated strike, truckers blocked the road infrastructure leading to and out of the most crucial ports where oil tankers unload the gasoline for the French market (Heusch 2016).

Technological risks for the logistical infrastructure can be further diversified into operational risks, which are directly caused by the usage of the particular infrastructure, and risks concerning the control and maintenance of the logistical infrastructures. A well-known example for an operational risk is the major explosion that hit the Chinese Port of Tianjin in 2016, caused by the handling of explosive goods, which forced the port to be entirely closed for two weeks (DB Schenker China 2015). A recent example for a technological risk caused by insufficient maintenance is the closure of the railway line traversing Germany from North to South in the vicinity of the town of Rastatt, as mentioned above.

Legal risks for critical logistical infrastructures include diplomatic restrictions and blockades as presented in the subsection on micro-political risks above. Furthermore, legal risks can be caused by a temporary or permanent blockade of a single infrastructural part or a whole region for national policy reasons. Finally, unforeseen and sudden changes to the legal framework for logistical operations can severely affect the infrastructure as a whole. A recent example for the latter is the so-called 'refugee crisis' in Europe, which is still ongoing and started approximately in 2015 as a result of the Syrian civil war. When millions of refugees sought shelter in Europe, various European countries, such as Hungary, Austria, Croatia, Serbia, France, and Austria, suddenly closed their borders or at least re-introduced regular border controls, which were formerly unknown within the common Schengen free trade region. Those policy changes, which happened overnight in some cases, led to traffic jams and delays of several days (Turner 2015). Another type of temporary regulatory change is introduced to protect certain events of particular risk. The Chinese city of Hangzhou, for example, was completely off-limits for all logistical transportation during the G20 summit for security reasons (Breakbulk 2016). On a few rare occasions, cities are even permanently cut off from logistical infrastructure by special checkpoints and protected by tightened entry regulations, such as the so-called 'Closed Cities' of Russia.

Ecological risks are risks caused by the natural environment. Such risks are diverse and often have dramatic effects on the logistical infrastructure. Low water levels, floods, earthquakes, typhoons, hurricanes, and other drastic environmental catastrophes regularly debilitate or close down whole road, inland waterway, and rail networks and prevent airplanes from operating. Most dramatically, the Nepali earthquakes of 2015 cut off a large part of Nepalese society from any form of logistical transportation, and thus from all supplies, for weeks (Page 2015). Less drastically, the eruption of the volcano Eyjafjallajökull in 2013 grounded thousands of airplanes across Europe for several days (Randelhoff 2010).

2.1 Categorization and Interdependencies

While the above PESTLE analysis might suggest that risks can be categorized into the described manner, they are in fact often highly interdependent or might fit well into several of the mentioned categories. One extreme example is the risks linked to the Bikini Atoll, which belongs to the Marshall Islands, an independent Pacific Island nation. Political risks, namely World War II and the following Cold War, led to an American interest in the Pacific region and in a national nuclear weapon program, which required a remote testing ground. The US government decided to use the Bikini Atoll as the test ground for its nuclear program, which led to environmental and, as a result of a large re-settlement program, to social risks. Thus, the single event 'nuclear testing in the Bikini Atoll' directly caused three different types of risks, showing how much the different categories can be interwoven. Guyer (2011) describes the whole Bikini Atoll nuclear testing disaster and its consequences in detail.

Similarly, especially as a result of ongoing digitalization, different infrastructures are increasingly interdependent. Today, a power outage has an impact on the IT infrastructure, which again has an impact on both the logistical and the freshwater supply infrastructure. Such indirect impacts of a power outage can thus always debilitate other, dependent, infrastructures, which might lead to secondary environmental and social risks. Rinaldi et al. (2001) summarize how different infrastructures are increasingly dependent on each other.

2.2 Existing Methodology

Only a limited number of publications have so far explicitly considered risks for critical logistical infrastructures. In the following, the few existing political and scientific approaches are summarized.

From a political perspective, risk management for critical infrastructures, in particular for logistical infrastructures, has its roots in the USA and can be divided into three eras. In a first era, the then President Bill Clinton introduced the term 'critical infrastructure' in 1996 formally by establishing the 'Commission on Critical Infrastructure Protection', which was set up to define a framework for risk management for critical infrastructures (see President's Commission on Critical Infrastructure Protection (1997)). Furthermore, the first report of the commission initially raised public awareness of the significance of national infrastructures for the welfare and quality of life for US-American citizens. Other national governments and international organizations did not initially adopt the terminology in that era. The suggestions of the commission and media reports focused on the protection of local infrastructures and the identification of criticalities of single links within the infrastructural networks. The overwhelming majority of the concerned risks in this era were thus environmental, operational, and technological risks.

The 9/11 terrorist attacks against the World Trade Center and the Pentagon started the second era of political interest in critical infrastructures. Disruptively, political actors around the world, led by North American and European policy makers, focused on the protection of national and international critical infrastructures. In this second era, nearly all institutional publications and studies focused on the risk of terrorist attacks, which had previously been largely ignored. Among others, Collier and Lakoff (2008) describe the shift of focus in great detail for the USA. Following the US-American role model, the United Nations (CTITF), the UK (CPNI), the European Union (EPCIP), and other political actors established specialized institutions for the risk management of critical infrastructures. While most of those institutions were originally founded to focus on the risk of terrorist attacks, they nearly all define holistic risk management for critical infrastructures as their institutional goal.

The third era, again, started with the realization of a, so far ignored, risk. In 2007, Estonia was hit significantly by the so-called 'Web War I'—a large-scale and coordinated hacker attack against all IT service of the Baltic country (see The Economist 2010). The ongoing attacks led to a full shutdown of all the Internet-based services in Estonia for a full week. Those services could only be restarted by disconnecting the Estonian Internet infrastructure from the international network for almost a month (Jackson 2013). As an institutional countermeasure to Web War I, NATO defined the 'Policy of Cyber Defense' in April 2008 and, subsequently, established the NATO Cooperative Cyber Defense Centre of Excellence (Herzog 2011). After more cyberattacks against the former Soviet States of Lithuania 2008, Georgia 2008, and Kazakhstan 2009, for all of which Russia was found responsible, the topic of 'cybersecurity' got even more into the focus of NATO. It was finally entirely interwoven with the thematical complex of infrastructure protection at a NATO ministerial conference with the topic 'critical infrastructures and cybersecurity' in April 2009 (Bumgarner and Borg 2009). As result of a perceived decreasing risk of terrorist attacks and an increased risk of cyberattacks from 2007/2008 on, the focus of the institutional work for protecting critical infrastructures subsequently shifted mainly to the protection of information infrastructures.

Recent events, like the activities of the so-called 'Islamic State', shift back the focus on the risks of terrorism and away from cyberthreats (Stock 2017).

The political and institutional eras of risk management for critical infrastructures reflect the 'Western World' view, which was led by the USA, Canada, and Europe. In other parts of the world, the above eras did not happen to the same extent. The People's Republic of China, for instance, still did not formally define the term 'critical infrastructure' or establish an institution that is responsible for protecting it. Other countries focus on risks that are most relevant for them. The British Virgin Islands, for example, focus entirely on environmental risks, like tornados (Penn 2010).

Scientifically, probably the first approach for the protection, or destruction, of a critical infrastructure was published by the US-American think-tank 'RAND Corporation', which mainly conducted contract research for the US Navy in the 1950s. The mathematician T. E. Harris specified, together with former general D. F. S. Ross, the so-called 'Maximum Flow Problem' in 1955 (Harris and Ross 1955), which became a classic optimization problem. That problem is solved to determine the maximal (one-dimensional) flow of goods within a network. Together with two other RAND Corporation members, L. R. Ford Jr. and D. R. Fulkerson, Harris developed the first efficient and exact procedure to solve this combinatorial problem. Furthermore, he discovered and proved the 'Max-Flow-Min-Cut Theorem', which observes that the maximum flow of a certain network has exactly the same value as the minimum cut of the same network. Since the publication of the work of Harris and Ross in 1999, it became clear how this seemingly theoretical work helped the US Navy in military planning. As a 'case study', Harris and Ross calculated the maximum flow of goods from the Soviet Far East to Eastern Europe through the Soviet railway network. Furthermore, the authors observed that a minimum cut would have the same value and made a proposal to military strategists how to calculate such a minimum cut for any possible network. This observation, linked with a remark within the publication, that 'airstrikes are an effective option to debilitate a railway network to prevent the transportation of troops and military equipment', showed why the US Airforce invested in this first-ever scientific research that identified critical infrastructures (Schrijver 2002).

The early research of the RAND Corporation founded an entire research topic, which is best described as 'search for the most critical edge(s).' As such a criticality measurement is most relevant for military applications, either for directed attacks or for an effective defense, this research field grew steadily during the Cold War (see, i.e., Wollmer 1963, 1964, 1968; Fulkerson and Harding 1977; Lubore et al. 1971; McMasters and Mastin 1970; Ratliff et al. 1975; Corley and Chang 1974; Golden 1977; Corley and Sha 1982; Malik et al. 1989 and Ball et al. 1989).

Shortly after the end of the Cold War, the tone and the applications of the research field changed instantly. Suddenly, the search for the most critical component of a network became a purely theoretical research topic and the problem was subsequently defined as 'Network Interdiction Problem' by Wood (1993).

Within the last decade, as a direct result of the increased political interest in the field, most publications focused on finding the most critical components of critical infrastructures. Brown et al. (2005, 2006) were the first to link both topics. In parallel, Salmerón et al. (2004, 2009) presented several approaches to identify the most critical component of an electric grid network. Church and Scaparra (2006) and Scaparra and Church (2008) used the same theoretical foundation to identify the criticality of single network components for the construction of a new facility.

Finally, Alderson et al. (2011) published the first scientific paper which focuses on identifying the critical infrastructure within a general logistical network.

In addition to those contributions from a rather analytical background, a few papers from a risk management perspective did consider risk management for critical infrastructures in particular. Sapori et al. (2014) proposed a generic analytical risk management methodology to manage risks of a critical infrastructure, while Avritzer et al. (2012) broadly show both the challenges and the limits of a systematic risk management for critical infrastructures.

Adar and Wuchner (2005) published an overview of the current state of risk management for critical infrastructure from a business perspective.

They emphasize the central importance of an extensive risk management for critical infrastructure for the success of any economic and public actor.

It can be observed that almost all of the mentioned scientific works on risk management for critical logistical infrastructures focus on the possible economic losses through a potential risk realization. However, it is important to emphasize that critical logistical infrastructures are not only relevant to businesses but are an integral part of the daily life of most citizens. Thus, a risk management for critical logistical infrastructures always has a large value for a society as a whole. To address such social effects of a debilitated logistical infrastructure, the World Bank established and spearheaded a scientific research branch called ‘Social Risk Management’, which is extensively described by Holtmann et al. (2001) and Holzmann et al. (2003) and critically questioned by Godfrey et al. (2009).

Finally, two often-cited publications discussing the scientific focus of risk management for critical infrastructures should be mentioned. Cardona (2004) tried to understand risk management for critical infrastructures as a holistic research topic and unite or cooperate between the various research fields, namely risk management, network theory, social sciences, and security sciences. Finally, Boin and McConnell (2007) discuss the limits of a risk management for critical infrastructures and link the field with resilience management, which tries to recover an infrastructure as soon as and as less cost-intensively as possible after a risk is realized.

3 Evaluation of Risks for Critical Logistical Infrastructures

3.1 Basic Assumptions

When we talk about logistical infrastructure, we include all relevant stationary facilities that are required to execute the basic logistical processes (i.e., transportation, handling, and warehousing). The logistical infrastructure contains roads, railways, inland waterways, pipelines, but also warehouses and transshipment points such as ports, airports, container terminals, and others.

The logistical infrastructure can be modeled as a network. The warehouses and transshipment points—or in general: the locations where handling, warehousing, and other logistical activities (often called ‘value-adding services’) take place—are modeled as vertices. Thus, each vertex $v \in V$ represents a logistical facility. On the other hand, the roads, railroads, inland waterways, and pipelines are modeled as edges. Each edge $e \in E$ represents a connection between two logistical facilities. Consequently, the whole logistical infrastructure is represented by the graph $G = (V, E)$.

We assume that for each vertex $v \in V$ and for each edge $e \in E$ the cost for using the specific vertex or edge is known. Thus, a value $c(v) \geq 0$ exists for every $v \in V$, and a value $c(e) \geq 0$ exists for every $e \in E$. This cost should be given as cost per shipping unit.

Our last assumption is that all shipments for a specified period are known a priori. The related shipment data contains at least the source and the sink, both defined as vertices $v \in V$. The shipment data must also contain information about the number of shipping units, so that the cost for a shipment can be calculated. The exact route for a shipment does not have to be given; we can assume that the route can easily be calculated by using established shortest path algorithms.

3.2 Evaluation Approach

The basic approach for evaluating risks for critical logistical infrastructures is based on one more assumption and an elementary cost comparison:

- We assume that there is an overall decision maker (e.g., a policy maker in a ministry or in another public authority) who needs to evaluate and prioritize risks for logistical infrastructures. The decision maker would then analyze one infrastructure element after another, evaluating the risks. In the end, all relevant infrastructure elements are evaluated and can be ranked by the implied consequences of risk events. (For simplicity reasons, we will focus on risks for vertices, such as ports and warehouses. However, the risk evaluation procedure can easily be transferred to all elements of the network including the edges.)
- For evaluating the risk for a certain element of the infrastructure, we will compare the total logistical cost for two specific situations. The 'normal' situation will be specified as a situation without any risks being realized. In such a situation, the total logistical cost C^{norm} will be calculated by the sum of the cost for each edge and for each vertex, if all orders are fulfilled. The situation 'under risk' will be specified as a situation, where (due to a risk being realized) a certain element of the logistical infrastructure is not usable, or the capacity is limited. In such a situation, shipments must be redirected using the remaining network. If the 'normal' situation is characterized by cost-optimal routes, the situation under risk will obviously lead to higher total logistical costs C^{risk}.
- The difference between the cost for the 'normal' situation and the situation under risk will be interpreted as the consequence if a risk for a certain vertex is realized: $\Delta C = C^{risk} - C^{norm}$.

3.3 Implementation

For the implementation of the evaluation approach, we will create an additional matrix A_v for each vertex $v \in V$ that should be evaluated. This matrix A_v only stores the information of the set of orders that are relevant for the evaluation process. This contains exactly those shipping orders O_v that use the specific vertex $v \in V$, which should be evaluated: $O_v = \{(v_1, w_1), \dots, (v_n, w_n)\}$. All other shipping orders are considered as irrelevant for the evaluation. In the matrix A_v, the source and sink vertex v_i and w_j for each order as well as the shipping quantity $q_{i,j}$ are saved. This leads to the definition of an element $(a_v)_{i,j}$ of the matrix A_v as $(a_v)_{i,j} = \begin{cases} q_{i,j} & \text{if } (v_i, w_j) \in O_v \\ 0 & \text{else} \end{cases}$.

The graph that represents the logistical infrastructure without the vertex (or vertices) that is affected by the risk event is noted as $\widehat{G} := G[V \backslash R] = \left(\widehat{V}, \widehat{E}\right)$ with $\widehat{V} = V \backslash R$ and $\widehat{E} = \{\, e = (v, w) \in E | v, w \in \widehat{V}\}$.

To calculate C^{norm} and C^{risk}, well-established shortest route algorithms can be applied. For each source/sink combination of the additional matrix A_v that uses the affected vertex, thus with $(a_{v^*})_{i,j} > 0$, the cost can be calculated by summing up the cost per used infrastructure element. This will be determined by multiplying the cost per shipping unit with the shipped quantity. For simplicity reasons, we assume that only edges induce cost. (Again, this assumption can easily be omitted.) The total logistics cost for shipping all orders that use the vertex v^* under normal conditions, thus without the risk realization, are calculated by $C_{v^*}^{norm} = \sum_{(i,j):(a_{v^*})_{i,j}>0} C_{i,j}$. The total logistics cost after the risk event affected vertex v^* is then calculated by $C_{v^*}^{\text{risk}} = \sum_{(i,j):(a_{v^*})_{i,j}>0} \widehat{C}_{i,j}$. In this case, the shortest route algorithms use the subgraph $\widehat{G} := G[V \backslash R] = \left(\widehat{V}, \widehat{E}\right)$.

Finally, the consequence of the risk affecting vertex v^* is calculated as the difference between the total cost of the normal situation and the total cost of the situation under risk, as mentioned above: $\Delta C = C^{risk} - C^{norm}$.

3.4 Strengths, Weaknesses, and Extensions

The evaluation approach presented in the previous sections is considered as a first step in developing a framework for risk evaluation of critical infrastructure. It is characterized by specific strengths, but it also shows room for development. In this section, we discuss such strengths and weaknesses and outline options for further progress.

The evaluation approach is meant to prioritize individual infrastructure elements by the quantified consequences implied by a realized risk event. The results reflect a ranking of infrastructure elements at risk and should be interpreted as a relative outcome and not, as might be expected, by their absolute values. With such results, decisions makers—especially in ministries on federal and regional level as well as institutions—receive relevant information and can focus the development of counteractive measures on those elements of the logistical infrastructure where a risk realization would lead to the highest overall consequences. The results thus lead to an efficient allocation of resources for an effective risk management. The approach can, on the other hand, not be used for evaluating a single element on its own by assignment of 'the real' cost of a risky event, i.e., the absolute value of all costs that are generated by the risk. Thus, the suggested evaluation approach is not intended to support decision makers on a local level, such as the manager of a single container terminal.

There is a second reason why the approach does not support managers on the element level, but policy makers on higher levels: A risk affecting an element of the infrastructure will lead to negative consequences, i.e., to additional cost, for the analyzed element. If shipments are redirected, they use other elements of the infrastructure. If the providers of the then used infrastructure can create additional revenues, they benefit from a risk that affects other elements. Only a policy maker on a higher level who has responsibility for the overall cost will be interested in the efficient allocation of resources for managing the risks, i.e., for minimizing the total risk-induced costs.

A necessary requirement for comparing risks for elements of the critical logistical infrastructure in the described way is that the risky events are specified identically. For example, a risk event for container terminals could be specified as a 24-hour interruption of all activities due to a breakdown of the power supply. To have a consistent risk evaluation and ranking, all considered terminals should be evaluated for a risk event with the same specification.

Another strength of the approach lies in its simplicity. For evaluating an element of the infrastructure, only the data of the infrastructure network and of those orders that use the specific element is required. This has two positive effects: On the one hand, data collection is relatively easy. If we assume that the cost of data retrieval depends on the amount of data that is necessary, also the cost of data provision is low. On the other hand, the calculation can be done in a short time. The computation time depends on the problem type and on the number of orders for which optimal routes must be calculated. Shortest path problems can be solved in polynomial time, so that the problem type does not lead to unacceptable computation time. By only considering those shipments that explicitly use the selected infrastructure element, the computation time is further reduced.

The simplicity of the approach leads, however, to weaknesses by excluding realistic assumptions. So far, the definition of risk event does not consider a recovery phase, where the capacity of the logistical infrastructure is continuously (maybe stepwise) increased over time, until the normal capacity is reached. Such dynamic processes could be implemented by either dividing the recovery time into discrete elements with increasing capacities and calculating the induced cost for each of the time frames or by applying a simulation approach. Also, the approach does not take into account possible buffers of whole shipments or shipping units in nodes of the logistical networks: As long as the storage capacity of a warehouse or any transshipment point allows for a temporary buffering, this option could be used to avoid re-routing a shipment.

Another weakness of the current implementation is the sole focus on transportation processes (including the implicit use of handling processes) without taking into account value-added services. The model can, however, easily be extended by modeling the possible or required logistical process for each element of the infrastructure.

The last weakness also results from the simplicity of the approach: In the current implementation, we assume that all shipments that use a certain infrastructure element can be re-routed without limitations. That is, the remaining infrastructure network provides enough capacity for all redirected shipments. This might not be the situation in reality: Due to absorbing redirected orders, the capacity of the then used infrastructure might reach its upper limit. This situation can be implemented by defining upper limits for the infrastructure network; the upper limits can take into account some average utilization to include an initial capacity usage. To include possible priorities of shipments, the approach can be extended by using not only the shipments that use the infrastructure element in focus, but all shipments. This way, penalty costs can be used to find an overall optimum, i.e., the cost-optimal routing of all orders minimizing total logistics cost including penalties.

The approach focuses only on the consequences of risky events but does not include the probabilities of those events. This is consistent, since the aim of the approach is to generate a ranking based on the consequences for certain events. Since the calculation for one single risk event and for one specific element of the infrastructure leads to a single result (the cost as the consequence of the risk event), the probabilities (if they can be assessed or estimated) can be used without problems, so that the usual risk parameters (consequence and probability) are considered for decision making.

A last aspect focuses on data availability. The assumption that shipping data is available (especially specifying source, sink, and shipping quantity) does hold for some elements of the infrastructure—but not for all. Usually, ASNs (advanced shipping notices) are sent in electronic form to the partners in a logistics chain, so that such shipping data with the listed data items is available not only for transportation companies, but also for container terminals and other transshipment points, i.e., for the vertices of the network. It is also true for edges of the railway network, because the traffic on the railway network is managed by an institution. On the other hand, the assumption does not hold for infrastructure elements, which do not have to be booked in advance, such as most road infrastructure. For those elements, traffic distribution models for cargo shipments can be used to derive the data, which might not be exact, but offers a reasonable precision for risk evaluation.

4 Summary and Outlook

A structured risk management for critical logistical infrastructures is becoming increasingly important for the most and the least developed countries in the world alike. The most developed logistical infrastructures, like the European road and rail networks, are starting to suffer increasingly from dilapidated and crumbling infrastructural assets, which increasingly require strategically planned maintenance prioritization. On the other hand, developing countries, like those in the Global South, are extending their own road and rail infrastructures rapidly, building thousands of road and rail kilometers every year, and thus have a strong need to strategically distribute funds to those regions that are currently most vulnerable to being completely cut off by the realization of any potential risk.

The approach presented in the previous section is an easy to implement way for how the risk evaluation phase can be carried out. It supports policy makers on regional and federal levels by creating relevant information on the risk-based ranking of elements of the critical logistical infrastructure. With the evaluation results, such policy makers can create an efficient allocation of resources so that risk management is effective.

Due to its simplicity, the approach has some inherent weaknesses. However, most of the weaknesses can be overcome by extending the model. This can be done by using more data, but also by implementing simulation modules that allow dynamic effects to be considered.

However, it should be noted that the current level of risk management for logistical infrastructure is on a relatively low level: Institutional, regular, and methodologically sound risk management is seldom carried out; thus, the maturity level of risk management is low. On the other hand, data to analyze risks in detail is often not available at all or only on an aggregate level that does not allow for a detailed analysis and evaluation of risk. Therefore, the suggested approach can lead to a large step forward in risk management for critical logistical infrastructure.

References

Abarez (2016). Artsakh determined to open Stepenakert airport for ‘people’s right to free movement, http://asbarez.com/141373/artsakh-determined-to-open-stepanakert-airport-for-peoples-right-to-free-movement/.

Adar, E., & Wuchner, A. (2005). Risk management for critical infrastructure protection (CIP) challenges, best practices & tools. In *First IEEE International Workshop on Critical Infrastructure Protection*.

Alderson, D. L., Brown, G. G., Carlyle, W. M., & Wood, R. K. (2011). Solving defender-attacker-defender models for infrastructure defense. In K. Wood & R. Dell (Eds.), *Operations research, computing and homeland defense* (pp. 28–49). Hannover, MD: Institute for Operations Research and the Management Sciences.

Avritzer, A., Di Giandomenico, F., Remke, A., & Riedl, M. (2012). Assessing dependability and resilience in critical infrastructures: challenges and opportunities. In K. Walter, A. Avritzer, M. Vieira & A. V. Moorsel (Eds.), *Resilience assessment and evaluation of computing systems* (pp. 41–63). Berlin, Heidelberg: Springer.

Ball, M. O., Golden, B. L., & Vohra, R. V. (1989). Finding the Most vital arcs in a network. *Operations Research Letters, 8*(2), 73–76.

Boin, A., & McConnell, A. (2007). Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience. *Journal of Contingencies and Crisis Management, 15*(1), 50–59.

Breakbulk (2016). G20 Summit impacts Hangzhou logistics. http://www.breakbulk.com/g20-summit-impacts-hangzhou-logistics/.

Brown, G. G., Carlyle, W. M., Salmeron, J., & Wood, K. (2005). Analyzing the vulnerability of critical infrastructure to attack and planning defenses. In H. Greenberg & J. Smith (Eds.), *INFORMS tutorials in operations research* (pp. 102–123). Hannover, MD: Institute for Operations Research and the Management Sciences.

Brown, G. G., Carlyle, W. M., Salmerón, J., & Wood, K. (2006). Defending critical infrastructure. *Interfaces, 36*(6), 530–544.

Bumgarner, J., & Borg, S. (2009). *Overview by the US-CCU of the Cyber campaign against Georgia in August of 2008*. US-CCU Special Report.

Cardona, O. D. (2004). The need for rethinking the concepts of vulnerability and risk from a holistic perspective: A necessary review and criticism for effective risk management. In G. Bankoff, G. Frerks, & D. Hilhorst (Eds.), *Mapping vulnerability: Disasters, development and people* (p. 17). London: Earthscan.

Church, R. L., & Scaparra, M. P. (2006). Protecting critical assets: The r-interdiction median problem with fortification. *Geographical Analysis., 39*(2), 129–146.

CNN (2003). *Ohio trucker joined al Qaeda Jihad*. http://edition.cnn.com/2003/LAW/06/19/alqaeda.plea/.

Collier, S., & Lakoff, A. (2008). The vulnerability of vital systems: How 'critical infrastructure' became a security problem. In: M. Dunn & K. Soby (Eds.), *Securing the homeland: Critical infrastructure, risk and security* (pp. 40–62). London: Routledge.

Corley, H. W., & Chang, H. (1974). Finding the n most vital nodes in a flow network. *Management Science, 21*(3), 362–364.

Corley, H. W., & Sha, D. Y. (1982). Most vital links and nodes in weighted networks. *Operations Research Letters, 1*(4), 157–160.

DB Schenker China (2015). *Explosions in industrial area in Tianjin impacts port operations*. http://www.dbschenker.com.cn/log-cn-en/news_media/news/9842348/explosion_in_tianjin.html.

Fulkerson, D. R., & Harding, G. C. (1977). Maximizing the minimum source-sink path subject to a budget constraint. *Mathematical Programming, 13*(1), 116–118.

Godfrey, P. C., Merrill, C. B., & Hansen, J. M. (2009). The relationship between corporate social responsibility and shareholder value: An empirical test of the risk management hypothesis. *Strategic Management Journal, 30*(4), 425–445.

Golden, B. (1977). A problem in network interdiction. *Naval Research Logistics Quarterly, 25*(4), 711–713.

Guyer, R. L. (2011). Radioactivity and rights—clashes at bikini atoll. *American Journal of Public Health, 91*(9), 1371–1376.

Harris, T. E., & Ross, F. S. (1955). *Fundamentals of a method for evaluating rail net capacities* (No. RM-1573). Santa Monica, USA: RAND CORP.

Heinrici, T. (2017). Rheintalbahn ab 2. Oktober wieder frei. https://www.dvz.de/rubriken/land/schiene/single-view/nachricht/rheintalbahn-ab-2-oktober-wieder-frei.html.

Herzog, S. (2011). Revisiting the Estonian cyber attacks: Digital threats and multinational responses. *Journal of Strategic Security, 4*(2).

Heusch, P. (2016). Streik und Straßenblockaden legen Teile des Landes lahm. http://www.swp.de/ulm/nachrichten/politik/streik-und-strassenblockaden-legen-teile-des-landes-lahm-13020619.html.

Holzmann, R., & Jørgensen, S. (2001). Social risk management: A new conceptual framework for social protection, and beyond. *International Tax and Public Finance., 8*(4), 529–556.

Holzmann, R., Sherburne-Benz, L., & Tesliuc, E. (2003). *Social risk management: The World Bank's approach to social protection in a globalizing world*. Washington DC, USA: World Bank.

Jackson, C. M. (2013). Estonian cyber policy after the 2007 attacks: Drivers of change and factors for success. *New Voices in Public Policy*, *7*(1).

Lubore, S. H., Ratliff, H. D., & Sicilia, G. T. (1971). Determining the most vital link in a flow network. *Naval Research Logistics Quarterly, 18*(4), 497–502.

Malik, K., Mittal, A. K., & Gupta, S. K. (1989). The k most vital arcs in the shortest path problem. *Operations Research Letters, 8*(4), 223–227.

McKenzie, S. (2016). *Brussels travel: Flights suspended, transit limited*. http://edition.cnn.com/2016/03/22/europe/brussels-explosions-transport-flights-metro-suspended/.

McMasters, A. W., & Mastin, T. M. (1970). Optimal interdiction of a supply network. *Naval Research Logistics Quarterly, 17*(3), 261–268.

Morley, N. (2013). *Bold plan to regenerate derelict Nicosia airport*. http://cyprus-mail.com/2013/09/22/bold-plan-to-regenerate-derelict-nicosia-airport/.

Page, P. (2015). *Nepal earthquake response challenges logistics experts*. http://www.wsj.com/articles/nepal-earthquake-response-challenges-logistics-experts-1430343036.

Penn, A. B. (2010). *The Virgin Islands climate change green paper.* Conservation and Fisheries Department and Ministry of Natural Resources and Labour.

President's Commission on Critical Infrastructure Protection (1997). Critical Foundations—Protecting America's Infrastructures. https://fas.org/sgp/library/pccip.pdf.

Randelhoff, M. (2010). Eyjafjallajökull—Die Auswirkungen in Europa und der ganzen Welt. http://www.zukunft-mobilitaet.net/849/analyse/eyjafjallajoekull-fazit-schaden-flugverkehr-global/.

Ratliff, D. H., Sicilia, G. T., & Lubore, S. H. (1975). Finding the n most vital links in flow networks. *Management Science, 21*(5), 531–539.

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems, 21*(6), 11–25.

Salmerón, J., Wood, K., & Baldick, R. (2004). Analysis of electric grid security under terrorist threat. *IEEE Transactions on Power Systems, 19*(2), 905–912.

Salmerón, J., Wood, K., & Baldick, R. (2009). Worst-case interdiction analysis of large-scale electric power grids. *IEEE Transactions on Power Systems, 24*(1), 96–104.

Sapori, E., Sciutto, M., & Sciutto, G. (2014). A quantitative approach to risk management in critical infrastructures. *Transportation Research Procedia, 3,* 740–749.

Scaparra, M. P., & Church, R. L. (2008). A bilevel mixed-integer program for critical infrastructure protection planning. *Computers & Operations Research, 35*(6), 1905–1923.

Schlesiger, C. (2017). 75 Millionen Euro Umsatzverlust wegen Rastatt-Sperrung. http://www.wiwo.de/unternehmen/dienstleister/deutsche-bahn-75-millionen-euro-umsatzverlust-wegen-rastatt-sperrung/20477114.html.

Schrijver, A. (2002). *Combinatorial optimization: Polyhedra and efficiency* (24th ed.) (pp. 166–169). Heidelberg: Springer Science & Business Media.

Sottilotta, C. E. (2013). *Political risk: Concepts, definitions*. Challenge. Working Paper Series. LUISS School of Government.

Stock, J. (2017). United Nations Security Council open debate on the protection of critical infrastructure against terrorist attacks. *Statement by Interpol*. https://www.interpol.int/content/download/34261/450506/version/1/file/Statement%20by%20Secretary%20General%20to%20the%20UNSC.pdf.

Turner, C. (2015). *Eurotunnel warns of lengthy delays due to 'migrant activity'*. http://www.telegraph.co.uk/news/uknews/11762469/Eurotunnel-suspends-passenger-services-because-of-migrant-activity-in-Calais.html.

Ukraine Today (2015). *Cyborgs vs. Kremlin*. http://cyborgs.uatoday.tv/.

US PIRG Education Fund (2009). *Private roads, public costs*. http://www.uspirg.org/sites/pirg/files/reports/Private-Roads-Public-Costs-Updated_1.pdf.

Uysal, O. (2014). *10 things to know about baku-Tbilisi-Kars Railway Project*. https://railturkey.org/2014/10/20/baku-tblisi-kars-railway/.

Watson, L. (2014). *Inside the ruins of Gaza's airport*. http://www.dailymail.co.uk/news/article-2730465/Inside-ruins-Gaza-s-airport-Photographs-transport-hub-named-honour-Yasser-Arafat-open-just-three-years-destroyed-neglect-war.html.

Wollmer, R. D. (1963). *Some methods for determining the most vital link in a railway network*. RAND Memorandum, RM-3321-ISA.

Wollmer, R. D. (1964). Removing arcs from a network. *Operations Research, 12*(6), 934–940.

Wollmer, R. D. (1968). Stochastic sensitivity analysis of maximum flow and shortest route networks. *Management Science, 14*(9), 551–564.

Wood, R. K. (1993). Deterministic network interdiction. *Mathematical and Computer Modelling, 17*(2), 1–18.

Zaman, A. (2016). U.S. air strikes destroy last Euphrates bridges in Deir Ez Zor. https://en.zamanalwsl.net/news/18649.html.

Chapter 8
Procedure Model for Supply Chain Digitalization Scenarios for a Data-Driven Supply Chain Risk Management

Florian Schlüter

1 Introduction

Many cases in the literature, e.g., Ericsson (Pfohl et al. 2015; Glas and Kleemann 2016), Toyota (Pettit et al. 2013), Land Rover (Tang and Tomlin 2008) and other Japanese automotive companies and computer manufacturers (Chopra and Sodhi 2014) have shown supply chain (SC) vulnerability has increased over the last years. As a result, supply chain risk management (SCRM) became a critical supply chain management (SCM) discipline due to the increasing number of events causing SC disruptions and to lower the impact of SC glitches (Hillman and Keltz 2007). Faisal et al. (2006) have empirically shown the benefit of information sharing of supply chain members to understand the different risks which could have an impact on the supply chain. Therefore, an SC-wide proactive risk management based on risk-related information transparency is required to increase the security of supply, decrease safety stocks and to lower costs for manufacturers and their customers (Chatfield et al. 2004; Christopher and Lee 2004). While supply chain risk (SCR) information has been identified as crucial, the importance of a company's information processing capability to its SCRM effort has received little attention in the literature (Fan et al. 2016). The integration of modern technologies into SCs leads to a smarter SCM, which combines multiple independent data analytics models, historical data repositories, and real-time data streams (Wang and Ranjan 2015). Available real-time information and data-processing tools bring new opportunities for companies to react more quickly to changing conditions within the supply chain (Güller et al. 2015). Due to this embedded intelligence, SCM moves from supporting decisions to delegating them and, ultimately, to predicting which decisions need to be made (Butner 2010). Using this available data from digitalized SC processes in SCRM leads to a smarter, data-driven SCRM. Reviewing the literature related to digitalization

F. Schlüter (✉)
Graduate School of Logistics, TU Dortmund University, Dortmund, Germany
e-mail: florian.schlueter@tu-dortmund.de

G. A. Zsidisin and M. Henke (eds.), *Revisiting Supply Chain Risk*, Springer Series in Supply Chain Management 7, https://doi.org/10.1007/978-3-030-03813-7_8

reveals that most publications present actual applications and less attention is paid to conceptual models which make digitalization manageable (Lu 2017). This chapter presents a procedure model supporting the management in developing and assessing SC process-oriented digitalization scenarios with a focus on risk prevention or reduction. The scenarios can then be used for concrete digitalization projects.

In Sect. 2, a research overview related to SCRM and digitalization will be described. Afterwards, the procedure model and its content will be developed in Sect. 3 and following subsections. The paper ends with a conclusion in Sect. 4.

2 Research Overview

For the model development, it is necessary to describe the underlying SCRM procedure and aspects of digitalization. To point out the necessity for the development of a procedure model, a research overview about existing models and frameworks in the context of digitalization and SCRM will be given.

Supply Chain Risk Management

SCRM can be seen as an emerging critical and cross-functional discipline between SCM, corporate strategic management and enterprise risk management (ERM) (Hillman and Keltz 2007; Zsidisin and Ritchie 2009). In their literature review, Ho et al. (2015) stated that the proposed definitions of SCRM usually focus on specific elements of SCRM and do not span the SCRM processes completely or differ in their SCRM methods and types of events. Given this, the author also follows Ho et al. (2015) in their definition of SCRM as: "an inter-organizational collaborative endeavour utilizing quantitative and qualitative risk management methodologies to identify, evaluate, mitigate and monitor unexpected macro- and micro-level events or conditions, which might adversely impact any part of a supply chain". The definitions of SCRM processes are also very diverse. A research overview explicitly describing models and frameworks of SCRM has been developed by Ponis and Ntalla (2016). de Oliveira et al. (2017) performed a similar approach by screening 27 publications for SCRM steps and comparing them with the ISO 31000-SCRM procedure (e.g., Curkovic et al. 2013). Based on their exhaustive literature review, the following SCRM stages will be taken into account: risk identification (identification of risks and sources); risk analysis (measurement of risk consequences and identification of risk factors); risk assessment (evaluation of risks); risk treatment (proposal of strategies and mitigation of risks) and risk monitoring (measurement of results, control of risks and ongoing improvement process).

Digitalization and Industry 4.0

A digitalized SC makes potential risks visible, allows companies to monitor material flows in real time and to develop future plans (Goh et al. 2013). The integration of cyber-physical systems (CPS) in existing or new SC processes leads to a convergence of the physical world and the virtual world (Wan et al. 2015). CPS are physical objects, equipped with embedded systems, sensors and actuators adding intelligence and the ability for self-control, cross-linking with other CPS and for interaction with their environment (Bischoff et al. 2015). Besides the term digitalization, there are other definitions in the literature with a similar meaning, like Industrial Internet, Internet of Things, Integrated Industry, Smart Industry, Smart Manufacturing and Industry 4.0 (I4.0) (Hermann et al. 2016). Especially, the term Industry 4.0 or Industrie 4.0 is widely used in the German-speaking literature and slowly makes its way into the Anglo-Saxon literature (e.g., Wan et al. 2015; Qin et al. 2016). The main characteristic of I4.0 is autonomization based on cross-linked systems which communicate with each other via the Internet (Roth 2016). The main drivers for the digitalization of SC processes are typically an increase in flexibility and reaction rate of industrial/logistic systems (ten Hompel and Henke 2017). Another perspective is to improve the SC robustness by using this available data from digitalized SC processes and CPS in SCRM. This approach is driving the digitalization process mentioned in this chapter.

Existing Models and Frameworks

A recent publication by Lu (2017) gives insights about the development of publication numbers of I4.0 literature into categories "Concepts and perspectives of Industry 4.0", "CPS-based Industry 4.0", "Interoperability of Industry 4.0" "Key technologies of Industry 4.0" and "Applications of Industry 4.0". They found out, "Concepts and perspectives of Industry 4.0" has the smallest number of publications (18), providing evidence that the number of approaches trying to make Industry 4.0 on the SC level operationalizable is limited. One general approach is the "Dortmund Management-Model for Industry 4.0" by Henke, which formalizes "work-clusters" for transforming value-creating activities into I4.0 (Henke et al. 2018). An SC-focused approach comes from Hermann et al. (2016) who describe necessary activities for creating digitalization scenarios for logistic processes. However, their approaches do not take risk in SCs into account. SCRM and digitalization-related frameworks can be found at Kirazli and Moetz (2015) and Schlüter and Sprenger (2016). Kirazli and Moetz (2015) have developed a four-phase framework for digitalizing processes from a risk management perspective. Their method has a focus on potential risks through the implementation of technologies. There is also a lack of evaluations of the benefits of digitalization. Due to that, Schlüter and Sprenger (2016) developed a five-phase framework for process-oriented digitalization of risk identification. The main weaknesses of their method are a superficial description of suitable methods and tools for the different framework phases, especially for "risk digitalization" and "digitalization scenario evaluation", and they focus only on SCR identification.

Until now, the author is not aware of any models connecting SCRM and Industry 4.0, for guiding managers in a structured process of developing and assessing process-oriented digitalization scenarios to create a data-driven SCRM in the long run.

3 Model Development

A procedure model is a procedural method or regulation describing how the activities and results of a project should be executed (Jenny 2007). The existing methods can be divided up according to the scope of change and potential risks emerging from using each method: process optimization, process re-engineering and process improvement. Process optimization is characterized by a relatively high scope of change and low risk. The goal is to transform existing processes into more efficient processes. On the other hand, process re-engineering also has a high scope of change but also a high risk due to its fast and radical changes to business processes, creating a turbulent environment in companies. Process improvement (continuous improvement process) has a low scope of change and low risk due to its small improvement steps which take place over a long period of time on an operational level (Becker 2008).

The author believes digitalization will lead to radical changes and thus an approach is needed which is based on supporting a higher scope of change. Because process re-engineering did not lead to the desired results people had hoped for in the past (Becker 2008), both concepts will be combined to merge the disruptive ideas of process re-engineering with the idea of "just" improving existing processes. Now, instead of simply improving an existing process, the project team has to question the existing process and think about innovative improvements explicitly focusing on digitalization activities. The result is a reference-procedure model for developing supply chain process-oriented digitalization scenarios which will be tailored to a procedure model in the context of SCRM (see Fig. 1). The final procedure model for developing and assessing digitalization scenarios for SCRM consists of six steps and is described in the following sections.

As described above, classic sequential models are not designed with the intention of moving back from one phase to the previous phase. To overcome this weakness and allow the project managers to adjust a previous phase if something does not fit,

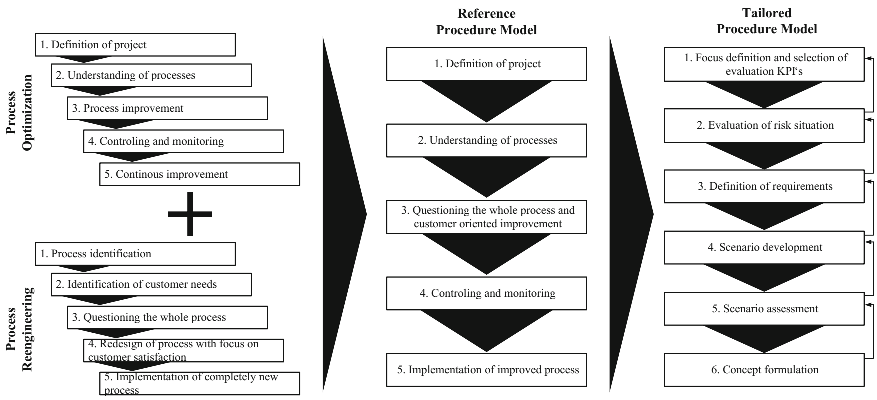


Fig. 1 Procedure model development

the phases will be modelled based on the modified waterfall with feedback model originally described by Royce (1970). Now it is possible to move back from one phase to the previous phase and to make corrections.

3.1 Focus Definition and Selection of Evaluation KPIs

At first, target processes (TP) in the SC have to be identified using data-collecting methods like process observation, expert interviews and secondary company data (Pawar 2004). It is necessary to focus on specific processes to digitalize the supply chain and migrate new technologies step by step. After completing a digitalization project, another part of the SC can be the focus of a new project. Another goal of this step is to define relevant KPIs for a later evaluation of the risk situation and digitalization scenarios. The KPIs should be chosen based on the KPIs used inside a company. One approach comes from Kuhn (1995), who defines five KPIs describing the state of each supply chain process: throughput time, technical capacity, work-in-progress, costs and schedule adherence (Kuhn 1995; Yüzgülec 2015).

When the object of observation as well as a set of KPIs are defined, the next step is to visualize the supply chain process and the existing risk management process for later discussion. A suitable method for modelling the existing risk management is the event-driven process chain (EPC), which is a flowchart for business process modelling that can also be used for business process improvements (Davis and Brabander 2007). Based on a comparative study by Nyhuis and Wiendahl (2009), the process chain model by Kuhn (1995) was especially developed for illustrating, designing and analysing logistic processes. The basic element of this model is a general process chain element, which is described in detail and influenced by the internal structures, processes, resources and steering modes as well as by exchange with the environment via a source and a sink (see Fig. 2) (Nyhuis and Wiendahl 2009).

Because a process chain element is always set up in the same way, independent of the level of particularization, it can be constructed for various levels of detail. An enterprise can be conceptualized en bloc as one process chain element or it can be broken down into various highly detailed levels (Nyhuis and Wiendahl 2009) (see example Fig. 3). The right level of detail must be estimated by the user.

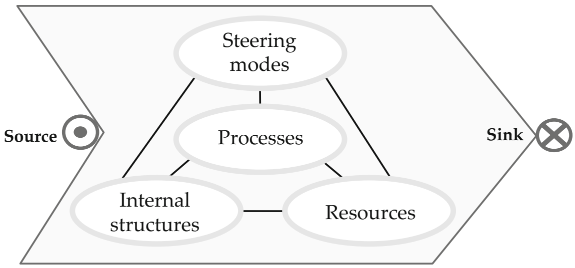


Fig. 2 Process chain element concept

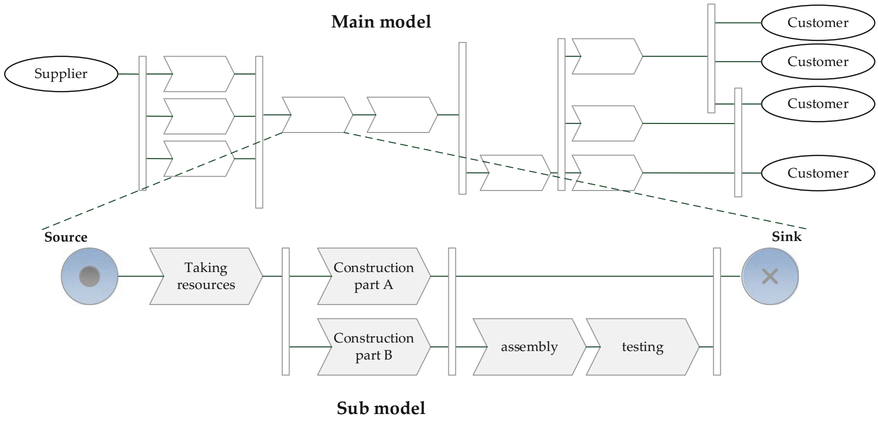


Fig. 3 Example supply chain visualization

3.2 Evaluation of the Risk Situation

The goal of this phase is to find, recognize and describe risk elements in terms of risk source, event and effect (ISO Guide 73 2009). Typical approaches for identifying risks for every defined process are: risk checklists, expert interviews and workshops (e.g., Häntsch and Huchzermeier 2013). It can be helpful to use the 5-Why method (asking five times "why" something happens) to dig deeper until the true root cause of a risk is identified (Serrat 2017). Afterwards, the processes and risk elements have to be put into relation by creating cause and effect chains (CEC), based on the Fault Tree logic (e.g., Lee et al. 1985). The CEC will be constructed for each process and later be merged to create an overall risk net. It is useful to start with potential risk sources. The risk sources have per definition no predecessor risk element (attention: this statement is only valid while focusing on only one process chain element—when creating the risk map later, risk sources of one element could also have predecessor risk elements in other parts of the process chain). After thinking about which of the expert's descriptions could be a source, the project manager has to think about what descriptions could be possible events resulting from these sources. In practice, there is no limit to risk events between risk sources and risk effects—it depends on the level of detail in the expert's description. It is also possible that one source can lead to different following events.

When all local CECs have been validated, they will be connected and integrated into a global risk net. This should happen in a workshop together with experts to easily identify risk dependencies between process chain elements. The final risk net contains all observed processes, related risks and inter-process risk dependencies.

After connecting risk effects and sources, the next step is to define the resulting effect on the process chain element, depending on the mitigation action chosen. For this step, some clarifications are necessary:

- The effects are measured on the aforementioned KPIs of the methodology by Kuhn (1995) and whenever an object leaves the process chain element (Yüzgülec 2015).
- Also, only the direct effects of a risk have to be considered and not subsequent effects. For example: Due to a risk event, a transport service provider has less transport capacity available, which leads to a rise in lead time—in this case, only the reduced capacity has to be considered because the rise in lead time will later be automatically considered within the simulative risk assessment.
- It is also possible that multiple effects occur. For example: Due to the bankruptcy of a service provider, a company has to switch to another provider which is more expensive and whose transportation is slower—in this case, there are two parallel effects, with a rise in cost and a rise in lead time which both have to be considered.

For the aggregated risk evaluation, a discrete event simulation (DES) will be combined with a Monte Carlo simulation (MCS), based on a methodology by Yüzgülec (2015). Simulation methods are recognized as a promising tool for detailed investigations and a supportive tool for the risk management process in supply chains (Güller et al. 2015). The DES simulates the regular material flow, based on the information from step 2 and the MCS is responsible for the consideration of risks and allows for a supply chain risk evaluation based on the loss distribution approach (LDA) (Shevchenko 2011). The probability of occurrence for each initial risk source and the impact of its corresponding risk effect(s) has to be quantified. For the LDA, risks will be quantified in terms of probability distributions. Based on operational risk literature (Shevchenko 2011), there are typically three sources to use for risk quantification: (1) company data; (2) external data and (3) expert knowledge (self-assessment). Self-assessment should be used if there is no or insufficient data available. In this case, the approach by van den Brink (2005) is recommended. At first, experts will be asked how often a certain risk occurs (during a time period or during order processing—depends on the case). If a risk occurs only once within a given period, the probability of occurrence can be assumed to be distributed binomially—or otherwise according to Poisson distribution (Cottin and Döhler 2013). Second, the risk impact has to be quantified. Due to the superficial description in Yüzgülec (2015) and also in van den Brink (2005), the author suggests the following approach for risk impact quantification: To fit expert knowledge to probability distributions which are usable within the simulation, the statistics software "R" is suggested, together with the package "rriskDistributions" (Belgorodski et al. 2017). The package helps to identify a suitable distribution based on two quantile values gathered from the experts. Usually, company experts are not statisticians and thus not able to provide detailed information about risk distributions (Steinhoff 2008). However, they are usually at least able to give information about the median risk impact (happens in 50% of the cases) and the pretty much worst impact they have experienced (considered as the 95 or 99% quantile). After selecting an appropriate distribution, the software will also give the user the relevant parameters for the simulation. The described approach makes it possible to assess the impact of multiple risks on single company process KPIs at the same time, as well as their individual impact on the whole system (sensitivity analysis). The results are presented as a distribution curve of the resulting KPIs and a Value-at-Risk can be identified based on the desired confidence interval. At the end of this step, the current situation is clear—the crucial supply chain processes and risk sources have been identified that can then be focused on in the following steps.

At this point, it has to be noted that as long as qualitative expert opinions are part of a quantitative evaluation, the results could be misleading as they could suggest an objectivity which is not really present. This must be considered when a decision is based on this evaluation.

3.3 Definition of Requirements for Future Supply Chain Risk Management

Before digitalization measures and scenarios can be created, it is necessary to define requirements for a future data-driven SCRM, considering the current SCRM procedure and risk situation (results from phase 1 and 2). These requirements serve as guidelines for the design phase. Right now, there is only a limited number of publications, describing the impact of digitalization on SCRM. Schlüter et al. (2017b) have screened available literature, based on a systematic review process to derive implications for each phase of an SCRM process but requirements cannot be defined solely on these implications. Recently the German acatech—National Academy of Science and Engineering—published a study to provide companies with I4.0 maturity stages to help them to identify their current I4.0 maturity stage and also to help achieve a higher stage in order to maximize the economic benefits of I4.0 and digitalization (Schuh et al. 2017). The maturity stages are described in Table 1 and should be considered when defining requirements.

The focus of I4.0 is usually on the technological aspects and the important role of CPS, but often neglected is the fact that CPS-based production systems are socio-technical systems consisting of a technical and social subsystem which are interlinked (Bostrom and Heinen 1977; Hirsch-Kreinsen 2014). The social subsystem focuses on the role of people using the technology while the technical subsystem focuses

Table 1 Industry 4.0 maturity stages (Schuh et al. 2017)

Maturity stage	Description
(1) Computerization	Support through IT-systems and worker will be disburdened from repetitive work
(2) Connectivity	Systems are structured and connected
(3) Visibility	Digital shadow available and management decisions are data-based
(4) Transparency	Companies understand why things happen
(5) Predictive capacity	Companies know what might happen and decisions are based on future scenarios
(6) Adaptability	Systems react and adapt autonomously

on the available technology and its role (Bostrom and Heinen 1977). This aspect should also be considered when defining requirements for a future SCRM system. To give support, Schlüter and Henke (2017) developed a framework for a workshop describing how SCRM will change over different I4.0 maturity stages. This framework serves as a basis for defining individual requirements for a desired SCRM maturity stage. The framework can be used to define individual and more detailed requirements for a specific use-case and desired maturity stage.

3.4 Scenario Development

Existing frameworks for developing digitalization scenarios (see Sect. 2) lack a detailed description of how the process should be undertaken or documented for later usage. They often only describe workshops as a method but give no explanation of what exactly should be discussed in the workshops or how to methodologically link or document the different domains discussed within the workshops (e.g., processes, weaknesses, and resources). An approach is needed to link identified risks with scenario aspects that have been developed and with current and future technologies so as to systematically create a concept.

Due to the high individuality of digitalization solutions, there is no way to take I4.0 off the rack so workshops are a suitable method for developing digitalization scenarios in a team. It is important that experts from the research field, as well as managers and creative employees from the shop floor all participate in the workshop.

An additional method is needed to structure the workshop and the results. The design structure matrix (DSM) method was originally developed by Steward (1962) to structure the analysis of a system of equations. Later he adopted his approach for the development of complex systems/products (Steward 1981). A DSM is a square matrix containing system elements that maps their relation to/interaction with each other (Danilovic and Browning 2007). Over the years, the areas of application have expanded from designing/analysing physical product architectures to process, organizational, project and software architectures (Browning 2016). The method has also been developed and, in addition to other forms, the domain-mapping matrix (DMM) method emerged (Danilovic and Browning 2007). While a square DSM only provides self-mapping of relationships among system elements within a single domain, an often but not necessarily rectangular DMM allows the mapping of elements from one domain with elements of another (Danilovic and Browning 2007). Because the participants in the workshops will discuss measures considering existing process risks (results step 3), stated requirements (results step 4) and existing and potentially useful technologies, the DMM method is suitable for structuring the workshop results. When discussing existing and potentially useful technologies it can help if the moderator provides a structured list of potential new technologies to support the creativity process. Such a list can be compiled by screening available literature, as described in Schlüter and Hetterscheid (2017).

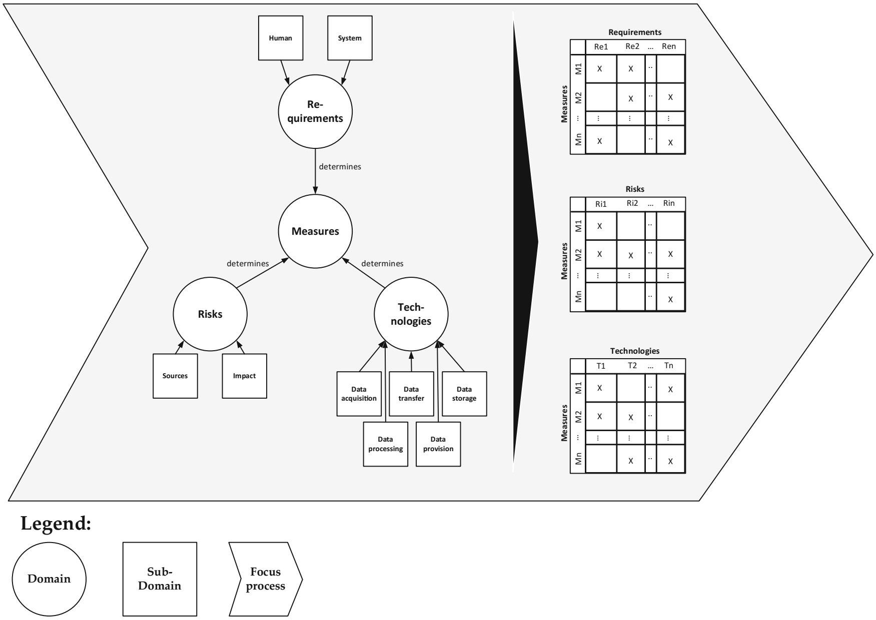


Fig. 4 Overview of domain relations and the resulting DMM

For each measure, it should be clear if it fits the stated requirements, if it lowers some of the risks and if it can be realized with technology already in use or with new technologies. Additional risks arising from one or more of the measures should also be added to the matrices. Because some of the measures might not be compatible with some of the other measures, multiple scenarios can be created and thus a set of the above-mentioned three DMMs has to be derived for each scenario (Fig. 4).

The use of DMM helps to structure the scenario development process and its results.

3.5 Scenario Assessment

The above-mentioned approaches (see Sect. 2) lack methodological support to evaluate the benefits of such scenarios especially with regard to SCRM. Aggregated assessment has only ever been carried out by Seiter et al. (2008), but the approach lacks objective cause and effect relationships. Thus, a new assessment approach will be proposed for an aggregated assessment of digitalization scenario benefits while considering risks in supply chains. The problem at this time is that limited empirical/objective information about digitalization benefits is available, and hence a method is needed which allows the estimation of costs and benefits of digitalization initiatives (Becker et al. 2016). This method should either be used with expert

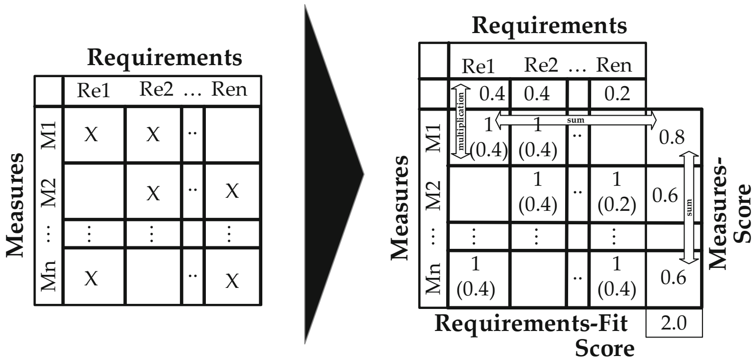


Fig. 5 Calculation of Requirements-Fit score

opinions or objective information (when available). As described, each scenario has a set of DMMs describing the relations between each measure and the risks, technologies and requirements. In the literature, DMMs can not only be used to describe binary relations between domains but also to describe the intensity of a relation via a numerical value (Maheswari et al. 2016). So, for each scenario, three evaluations have to be made which can later be used to compare scenarios based on Requirements-Fit, Risk-Improvement and Investment-Value categories.

Requirements-Fit

The Requirements-Fit score is relevant for identifying scenarios that lower risks, frequently with low-cost solutions but do not really fulfil the desired requirements in the long run. The starting point for the Requirements-Fit is the DMM with the measures and requirements domains.

To calculate the Requirements-Fit score, a weighted scoring model is suggested. Such a model provides a systematic process for selecting projects/scenarios (Lessard and Lessard 2007). At first, the requirements can be weighted in percentages so that in total they add up to 100%. After that the Requirements-Fit score can be calculated. When a measure has no relation to a requirement, the corresponding field gets ranked as 0 and when a measure fulfils a requirement it is ranked as 1. The last step is to multiply each score with the corresponding weights and the resulting products are added to get the total weight's score for each measure (Lessard and Lessard 2007). The project score results from adding all measure scores (Fig. 5).

Risk-Improvement

The evaluation of the Risk-Improvement is based on a further approach developed by Schlüter et al. (2017a) and expands the model from step 2 (risk assessment). For the Risk-Improvement, a scale starting with 0% and ending with 100% is suggested. In this case, 0% means that a risk is not affected by a bundle of measures, while 100% means a measure removes a risk source or effect completely. For each scenario, a

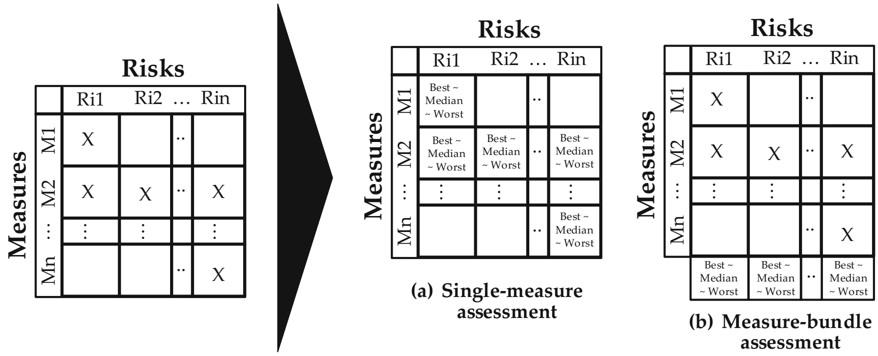


Fig. 6 Estimation of Risk-Improvement

group of experts has to assess what impact they think a measure will have on each risk (source and/or effect). This is done by having them describe the median measure impact (will probably happen in 50% of the cases) and the best as well as the worst impact they can think of (considered as the 5 or 95% quantile). To make it easier for the experts, specific intervals are suggested (e.g., 0, 25, 50, 75 and 100%). The assessment can be made for each Measure–Risk combination (more detailed but also more difficult to make a valid estimation) or for a bundle of measures for each risk (less detailed but easier to assess by experts) (Fig. 6).

Afterwards, the results have to be analysed with the help of the statistics software "R". For each risk source and/or effect, a distribution and its parameters can be derived from the expert opinions, similar to those from step 2.

These distributions can be used inside the risk assessment model and its Monte Carlo component (see Sect. 3.2) based on the formulas:

- $\text{Probability}_{\text{New}} = \text{Probability}_{\text{Old}} \times (1 - \text{Risk-Improvement}_{\text{Probability}})$
- $\text{Impact}_{\text{New}} = \text{Impact}_{\text{Old}} \times (1 - \text{Risk-Improvement}_{\text{Impact}})$

This helps to diminish the inherent uncertainty in the decision-making process and achieves results closer to reality (Zio 2013). The MC samples the possible combinations of parameters in proportion to their probability of occurring (Milanovic et al. 2010). As a result, in each simulation run, the stochastic risk parameters will be randomly chosen as well as the stochastic Risk-Improvement parameters and a new risk value will be calculated. The approach described allows the impact of multiple risks and measures on single company process KPIs to be assessed at the same time as well as their individual impact on the whole system (sensitivity analysis). The method that has been developed also makes it possible to assess DSs simultaneously with risks, which will not be directly affected by the DS and also with potential risks arising from the SC digitalization. The resulting Values-at-Risk can be compared with those from step 3 to determine the change from the current situation.

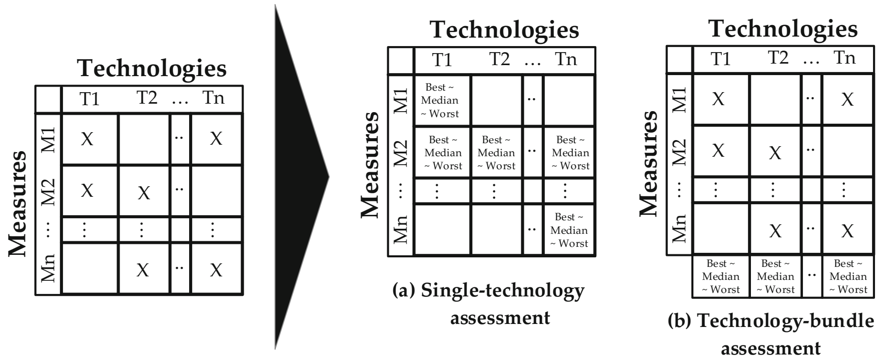


Fig. 7 Estimation of costs

Investment-Value

After calculating the Requirements-Fit and Risk-Improvement values for each scenario, it is useful to calculate the expected Investment-Value and its distribution using a Monte Carlo simulation, as practised in project cost estimation (Kwak and Ingall 2007). At this point, the DMM for measures and technologies is helpful. For each scenario, a group of experts has to fill out the matrix with their estimations of how much each measure will cost, based on the related technologies which have to be modified or installed. This happens by them having to describe the median costs (will probably happen in 50% of the cases) and the best as well as the worst cost they can think of (considered as the 5 or 95% quantile). They can do it either top-down (estimating the total costs for one measure or technology and then breaking it down to its components) or bottom-up (estimating the costs for each measure and technology relation and then checking if the total value fits to the experiences of the expert) (Fig. 7).

Afterwards, the matrices have to be analysed with the help of the statistics software “R”. For each relation, a distribution and its parameters can be derived from the expert opinions. These distributions can then be used in a Monte Carlo simulation to calculate a distribution of the expected total costs (Kwak and Ingall 2007).

All three value categories can be used to compare different scenarios with each other. By suggesting a DMM-based qualitative scoring, combined with a simulation-based risk and investment analysis, a methodology is presented to evaluate digitalization scenarios in SCRM. At this point, it has to be noted that this evaluation approach must be critically questioned in the same way as the risk evaluation in part 3 of the procedure model. As long as qualitative expert opinions are part of a quantitative evaluation, the results could be misleading as they could suggest an objectivity which is not really present. This must be considered when a decision has to be made. By collecting and integrating information from multiple sources, triangulation is a possible way to improve the risk assessment as well as the scenario-assessment process.

3.6 *Concept Creation*

Based on the structured documentation in step 4 and after the evaluation in step 5, a concept can be created. This concept describes the desired changes in each supply chain process, based on the desired requirements from step 3. On the basis of these changes, a future SCRM system can be conceptualized.

Outputs of this phase can be a rough architecture (e.g., Biswas and Sen 2016) based on the technologies used for each scenario and a project roadmap containing all information collected from the previous phases (object of observation, supply chain map, risk maps, risk evaluations, requirements, workshop results, scenario assessment results, drawn concept), time frame, documentation, strategic milestones, project leader and sponsor (Bode et al. 2014).

4 Conclusion

This chapter presents a novel approach to structuring a digitalization scenario development process and making it usable in an SCRM context. As a result, the new procedure helps to identify the current risk situation in a company and to define goals/requirements for a future data-driven SCRM. Based on these requirements and the current situation, digitalization measures and scenarios can be developed within workshops and supported by DMMs. Afterwards, scenarios can be evaluated based on three categories and a selected scenario can be further detailed to create a concept and roadmap for a subsequent implementation project.

Limitations and Further Research

When applying the procedure model, the user has to be aware of the fact that especially the simulation-based methods in the model need high user competence regarding DES and it takes time to collect all the data and to create a valid simulation model. In cases where there is only limited data available, alternative and more qualitative methods for risk and digitalization scenario assessment should be used. However, right now, only simulation-based methods can sufficiently consider the relations between risks and other risks as well as supply chain entities (Götze and Mikus 2015).

Especially, when it comes to scenario evaluations, empirical data is scarce and estimations are necessary. The user has to be aware that the estimated effects, in particular, are very speculative due to a lack of use-cases. While the Requirement-Fit values will still be highly subjective in the future due to the individually created requirements and measures, it can be expected that the Risk-Improvement and Investment-Value figures can be derived from existing use-cases in the future.

However, the procedure model and its methods which are presented here are a first approach to structuring the emerging, under-developed and highly diverse research field of I4.0 (Pfohl et al. 2015; Glas and Kleemann 2016). As a next step, the model should be applied to a use-case to show its applicability and a subsequent model for structuring the implementation process should be developed.

References

Becker, T. (2008). *Prozesse in Produktion und Supply Chain optimieren*. Berlin, Heidelberg: Springer.

Becker, W., Ulrich, P., Botzkowski, T., & Eurich, S. (2016). Controlling von Digitalisierungsprozessen - Veränderungstendenzen und empirische Erfahrungswerte aus dem Mittelstand. In R. Obermaier (Ed.), *Industrie 4.0 als unternehmerische Gestaltungsaufgabe: Betriebswirtschaftliche, technische und rechtliche Herausforderungen* (pp. 97–118). Wiesbaden: Springer Gabler.

Belgorodski, N., Greiner, M., Tolksdorf, K., & Schueller, K. (2017). *Package 'rriskDistributions'*. Online: https://cran.r-project.org/web/packages/rriskDistributions/rriskDistributions.pdf (08.11.2018).

Bischoff, J., Taphorn, C., Wolter, D., Braun, N., Fellbaum, M., Goloverov, A., et al. (2015). Erschließen der potenziale der anwendung von "Industrie 4.0" im Mittelstand. Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi). Mühlheim (Ruhr): Agiplan GmbH.

Biswas, S., & Sen, J. (2016). A proposed architecture for big data driven supply chain analytics. *International Journal of Supply Chain Management, 3*(2016), 7–34.

Bode, M., Schönhärl, J., Jager, M., & Schmidt, M. (2014). Innovationssysteme zur strategischen Steuerung von Innovationen. In F. Keuper & R. Sauter (Eds.), *Unternehmenssteuerung in der produzierenden Industrie* (pp. 67–88). Wiesbaden: Springer Fachmedien.

Bostrom, R. P., & Heinen, J. S. (1977). MIS problems and failures: A socio-technical perspective: Part I: The causes. *MIS Quarterly, 1*(3), 17–32.

Browning, T. R. (2016). Design structure matrix extensions and innovations: A survey and new opportunities. *IEEE Transactions on Engineering Management, 63*(1), 27–52.

Butner, K. (2010). The smarter supply chain of the future. *Strategy & Leadership, 38*(1), 22–31.

Chatfield, D. C., Kim, J. G., Harrison, T. P., & Hayya, J. C. (2004). The bullwhip effect: Impact of stochastic lead time, information quality and information sharing: A simulation study. *Production and Operations Management, 13*(1), 340–353.

Chopra, S., & Sodhi, M. S. (2014). Reducing the risk of supply chain disruptions. *MIT Sloan Management Review, 55,* 73–80.

Christopher, M., & Lee, H. (2004). Mitigating supply chain risk through improved confidence. *International Journal of Physical Distribution & Logistics Management, 34*(5), 388–396.

Cottin, C., & Döhler, S. (2013). *Risikoanalyse: Modellierung, Beurteilung und Management von Risiken mit Praxisbeispielen* (2nd ed.). Studienbücher Wirtschaftsmathematik. Wiesbaden: Springer.

Curkovic, S., Scannel, T., & Wagner, B. (2013). ISO 31000:2009—Enterprise and supply chain risk management: A longitudinal study. *American Journal of Industrial and Business Management, 3*(7), 614–630.

Danilovic, M., & Browning, T. R. (2007). Managing complex product development projects with design structure matrices and domain mapping matrices. *International Journal of Project Management, 25*(3), 300–314.

Davis, R., & Brabander, E. (2007). *ARIS design platform: Getting started with BPM*. London: Springer.

de Oliveira, U. R., Marins, F. A. S., Rocha, H. M., & Salomon, V. A. P. (2017). The ISO 31000 standard in supply chain risk management. *Journal of Cleaner Production, 151*(2017), 616–633.

Faisal, M. N., Banwet, D. K., & Shankar, R. (2006). Supply chain risk mitigation: Modeling the enablers. *Business Process Management, 12*(4), 535–552.

Fan, H., Cheng, T. C. E., Li, G., & Lee, P. K. C. (2016). The effectiveness of supply chain risk information processing capability: An information processing perspective. *IEEE Transactions on Engineering Management, 63*(4), 414–425.

Glas, A. H., & Kleemann, F. C. (2016). The impact of industry 4.0 on procurement and supply management: A conceptual and qualitative analysis. *International Journal of Business and Management Invention, 5*(6), 55–66.

Goh, R. S. M., Wang, Z., Yin, X., Fu, X., Ponnambalam, L., Lu, S., et al. (2013). RiskVis: Supply chain visualization with risk management and real-time monitoring. In *IEEE International Conference on Automation Science and Engineering (CASE), 2013* (pp. 207–212). August 17–20, 2013, Madison, WI, USA. IEEE, Piscataway, NJ.

Götze, U., & Mikus, B. (2015). Der Prozess des Risikomanagements in Supply Chains. In C. Siepermann, R. Vahrenkamp, & D. Siepmann (Eds.), *Risikomanagement in Supply Chains: Gefahren abwehren, Chancen nutzen, Erfolg generieren* (2nd ed., pp. 29–59). Berlin: Erich Schmidt Verlag.

Güller, M., Koc, E., Hegmanns, T., Henke, M., & Noche, B. (2015). A simulation-based decision support framework for the real-time supply chain risk management. *International Journal of Advanced Logistics, 4*(1), 17–26.

Häntsch, M., & Huchzermeier, A. (2013). Identifying, analyzing, and assessing risk in the strategic planning of a production network: The practical view of a German car manufacturer. *Journal Management Control, 24*(2), 125–158.

Henke, M., Besenfelder, C., Kaczmarek, S., Hetterscheid, E., & Schlüter, F. (2018). Dortmund management model—a contribution to digitalization in logistics and supply chain management. In *Proceedings of the 9th International Scientific Symposium on Logistics: ISSL 18* (pp. 113-124). June 13–14, 2018, Magdeburg, Germany.

Hermann, M., Pentek, T., & Otto, B. (2016). Design principles for Industrie 4.0 scenarios. In T. X. Bui & R. H. Sprague (Eds.), *Proceedings of the 49th Annual Hawaii International Conference on System Sciences* (pp 3928–3937). January 5–8, 2016, Kauai, Hawaii. IEEE, Piscataway, NJ.

Hillman, M., & Keltz, H. (2007). Managing risk in the supply chain—a quantitative study. Online: http://www.scrlc.com/articles/AMR_Managing_Risk.pdf (08.11.2018).

Hirsch-Kreinsen, H. (2014). Wandel von Produktionsarbeit - "Industrie 4.0". *WSI Mitteilungen, 6,* 421–429.

Ho, W., Zheng, T., Yildiz, H., & Talluri, S. (2015). Supply chain risk management: A literature review. *International Journal of Production Research, 53,* 5031–5069.

ISO Guide 73. (2009). *Guide 73: Risk management—Vocabulary.* ISO, Genf.

Jenny, B. (2007). *Project management: Knowledge for a successful career*. Zürich: Vdf Hochschulverlag.

Kirazli, A., & Moetz, A. (2015). A methodological approach for evaluating the influences of Industrie 4.0 on risk management of the goods receiving area in a German automotive manufacturer. In: *22nd EurOMA Conference: Operations Management for Sustainable Competitiveness.*

Kuhn, A. (1995). *Prozessketten in der Logistik: Entwicklungstrends und Umsetzungsstrategien*. Dortmund: Verlag Praxiswissen.

Kwak, Y. H., & Ingall, L. (2007). Exploring Monte Carlo simulation applications for project management. *Risk Managment, 9*(1), 44–57.

Lee, W. S., Grosh, D. L., Tillman, F. A., & Lie, C. H. (1985). Fault tree analysis, methods, and applications—A review. *IEEE Transactions on Reliability, 34*(3), 194–203.

Lessard, C. S., & Lessard, J. P. (2007). *Project management for engineering design*. Texas: Morgan & Claypool Publishers.

Lu, Y. (2017). Industry 4.0: A survey on technologies, applications and open research issues. *Journal of Industrial Information Integration, 6*(2017), 1–10.

Maheswari, J. U., Charlesraj, V. P. C., Kumar, G. S., & Padala, S. S. (2016). A study on assessment of non-conformances using multiple domain matrix: A case study from metro projects. *Procedia Engineering, 145,* 622–629.

Milanovic, D. L., Milanovic, D. D., & Misita, M. (2010). The evaluation of risky investment projects. *FME Transactions, 38,* 103–106.

Nyhuis, P., & Wiendahl, H.-P. (2009). *Fundamentals of production logistics: Theory, tools and applications*. Berlin, Heidelberg: Springer.

Pawar, M. (2004). *Data collecting methods and experiences: A guide for social researchers*. Elgin, Berkshire, New Delhi: New Dawn Press.

Pettit, T. J., Crocton, K. L., & Fiksel, J. (2013). Ensuring supply chain resilience: Development and implementation of an assessment tool. *Journal of Business Logistics, 34*(1), 46–76.

Pfohl, H.-C., Yahsi, B., & Kurnaz, T. (2015). The impact of Industry 4.0 on the supply chain. In W. Kersten, T. Blecker, & C. M. Ringle (Eds.), *Sustainability in logistics and supply chain management: New designs and strategies* (pp. 31–58). Berlin: epubli GmbH.

Ponis, S. T., & Ntalla, A. C. (2016). Supply chain risk management frameworks and models: A review. *International Journal of Supply Chain Management, 5,* 1–11.

Qin, J., Liu, Y., & Grosvenor, R. (2016). A categorical framework of manufacturing for Industry 4.0 and beyond. *Procedia CIRP, 52*(2016), 173–178.

Roth, A. (2016). Industrie 4.0—Hype oder Revolution? In A. Roth (Ed.), *Einführung und Umsetzung von Industrie 4.0: Grundlagen, Vorgehensmodell und Use Cases aus der Praxis* (pp. 1–15). Berlin, Heidelberg: Springer.

Royce, W. W. (1970). Managing the development of large software systems. In *Proceedings, IEEE Wescon* (pp. 1–9).

Schlüter, F., Hetterscheid, E., & Henke, M. (2017a). A simulation-based evaluation approach for digitalization scenarios in smart supply chain risk management. *Journal of Industrial Engineering and Management Science, 2017*(1), 179–206.

Schlüter, F., Diedrich, K., & Güller, M. (2017b). Analyzing the impact of digitalization on supply chain risk management. In *2017 IPSERA Conference.*

Schlüter, F., & Henke, M. (2017). Smart supply chain risk management—A conceptual framework. In: W. Kersten, T. Blecker, & C. M. Ringle (Eds.), *Digitalization in supply chain management and logistics* (pp. 361–380). Berlin: epubli GmbH.

Schlüter, F., & Hetterscheid, E. (2017). Supply chain process oriented technology-framework for Industry 4.0. In W. Kersten, T. Blecker, & C. M. Ringle (Eds.), *Digitalization in supply chain management and logistics* (pp. 275–299). Berlin: epubli GmbH.

Schlüter, F., & Sprenger, P. (2016). Migration framework for decentralized and proactive riskidentification in a Steel Supply Chain via Industry 4.0 technologies. In: A. Spyridakos & L. Vryzidis (Eds.), *Conference Proceedings of the 5th International Symposium and 27th National Conference on Operational Research*, Athens (pp. 85–91).

Schuh, G., Anderl, R., Gausemeier, J., ten Hompel, M., & Wahlster, W. (2017). *Industrie 4.0 maturity index: Managing the digital transformation of companies. acatech STUDY.* München: Herbert Utz Verlag.

Seiter, M., Isensee, J., & Rosentritt, C. (2008). Evaluation of RFID investment—The extended performance analysis (EPA) approach. In RFID *Systems and Technologies (RFID SysTech), 2008: 4th European Workshop on RFID Systems and Technologies* (pp. 1–6). June 10–11, 2008 in Freiburg, Germany, Institute of Computer Science and Social Studies (IIG). VDE-Verl., IEEE, Berlin u.a.

Serrat, O. (2017). *Knowledge solutions*. Singapore: Springer.

Shevchenko, P. V. (2011). *Modelling operational risk using Bayesian inference*. Berlin, Heidelberg: Springer.

Steinhoff, C. (2008). *Quantifizierung operationeller Risiken in Kreditinstituten: Eine Untersuchung unter besonderer Berücksichtigung von Szenarioanalysen im Rahmen von Verlustverteilungsmodellen*. Göttingen: Cuvillier Verlag.

Steward, D. V. (1962). On an approach to techniques for the analysis of the structure of large systems of equations. *SIAM Review, 4*(4), 321–342.

Steward, D. V. (1981). The design structure system: A method for managing the design of complex systems. *IEEE Transactions on Engineering Management EM, 28*(3), 71–74.

Tang, C., & Tomlin, B. (2008). The power of flexibility for mitigating supply chain risks. *International Journal of Production Economics, 116*(1), 12–27.

ten Hompel, M., & Henke, M. (2017). Logistik 4.0—Ein Ausblick auf die Planung und das Management der zukünftigen Logistik vor dem Hintergrund der vierten industriellen Revolution. In B. Vogel-Heuser, T. Bauernhansl, & M. Hompel ten (Eds.), *Handbuch Industrie 4.0 Bd.4: Allgemeine Grundlagen* (2nd ed., pp. 249–259). Berlin, Heidelberg: Springer.

van den Brink, G. J. (2005). Quantifizierung operationeller Risiken - Ein Weg zur Einbettung in den Management-Zyklus. In F. Romeike (Ed.), *Modernes Risikomanagement* (pp. 255–268). Weinheim: Wiley-VCH.

Wan, J., Cai, H., & Zhou, K. (2015). Industrie 4.0: Enabling technologies. In: *Proceedings of 2015 International Conference on Intelligent Computing and Internet of Things: ICIT 2015* (pp. 135–140). January 17–18, 2015, Harbin, China. IEEE, Piscataway, NJ.

Wang, L., & Ranjan, R. (2015). Processing distributed internet of things data in clouds. *IEEE Cloud Computing, 2*(1), 76–80.

Yüzgülec, G. (2015). *Aggregierte Bewertung von Risikoursachen in Supply Chains der Automobilindustrie*. Dortmund: Verlag Praxiswissen.

Zio, E. (2013). *The Monte Carlo simulation method for system reliability and risk analysis. Springer Series in Reliability Engineering*. London: Springer.

Zsidisin, G. A., & Ritchie, B. (2009). Chapter 1: Supply chain risk management—Developments, issues and challenges. In G. A. Zsidisin & B. Ritchie (Eds.), *Supply chain risk: A handbook of assessment, management, and performance* (pp. 1–12). Boston: Springer, US.

Chapter 9
Preparing for the Worst

Yossi Sheffi

1 Preparing for the Worst

In 2011, a decade after he helped co-found the Institute for Supply Chain Risk Management (ISCRIM), Bob Ritchie said, “In the past, risk was just accepted. Now companies are trying to identify what the risk drivers are and their consequences” (Zurich 2011a). The twenty-first century has seen growing academic research and corporate investment in SCRM as more leaders have come to see the power and perils of supply chains (Sheffi 2005, 2015). Business continuity has grown in importance in this connected world. At the same time, deep, broad, and lean supply networks have increased companies’ exposure to disruptions occurring at remote suppliers and customers. Events such as 9/11 in 2001, hurricane Katrina in 2005, the financial crisis in 2008, the Iceland volcanic eruptions of 2010, the Tohoku earthquake in 2011, and innumerable other natural, industrial, and human disasters have proven how risk ripples through companies, supply chains, and economies. “I have 14,000 suppliers. I guarantee that with 14,000 suppliers, at least one of them is not performing well today,” said Tom Linton, chief procurement and supply chain officer at Flextronics (Linton 2012).

Beyond qualitative awareness of the need for SCRM is the need for quantitative frameworks for making sensible investments in SCRM both at the aggregate enterprise level and at finer levels of granularity such as products, facilities, and customers. This implies quantifying both supply chain risks and investments that address supply chain risks. Most definitions of risk use three attributes: likelihood of the occurrence of a particular event or outcome; consequences of the particular event or outcome occurring; and the causal pathway leading to the event (Ritchie and Brindley 2007). The first two quantitative attributes define a probability

Y. Sheffi (✉)
Civil and Environmental Engineering, MIT Center for Transportation and Logistics, MIT, Cambridge, USA
e-mail: sheffi@mit.edu

G. A. Zsidisin and M. Henke (eds.), *Revisiting Supply Chain Risk*, Springer Series in Supply Chain Management 7, https://doi.org/10.1007/978-3-030-03813-7_9

distribution of outcomes while the third attribute defines the likely organizational scope and dynamics of contingent risk events. This likelihood, consequence, causal pathway model can be used to design SCRM investments and to evaluate the uncertain value of these investments to the enterprise.

2 Real Options: The Value of Preparation

The concept of a financial stock option provides an analytic framework for evaluating investments with uncertain payoffs such as those associated with preparing for disruption response. Real options (Trigeorgis 1995) are tangible assets that give the owner of the option the right, but not the obligation, to take a particular action in the future. For example, extra inventory in a warehouse or the spare capacity in a factory is a real option giving the company the right to utilize that spare stock or extra capacity during a supply disruption or a surge in demand. Without an upfront investment in the spare inventory or capacity, the company might face a shortage during a disruption.

2.1 Options' Valuation

Real options have two defining elements: a known upfront cost of creating the option (e.g., the capital cost of spare factory capacity or the cost of training and drilling) and an unknown net payoff that is contingent on some uncertain future event (e.g., the value of mitigation, recovery, or continuity if the option is exercised during a disruption). The mathematics of real options weighs the uncertain benefits of being able to exercise the option in the future against the certain costs of creating it in the present. The model considers the statistical likelihood of the benefit over time and the cost of the money over the time period when the option is available.

The specific analytical methods to evaluate real options are beyond the scope of this chapter,[1] but the general results are clear. If the likelihood of needing an option is high enough or if the payoff from having the option, relative to its cost, is high enough, then the option will be worth the investment. Most crucially, the value of having an option increases if volatility increases, be it demand volatility or supply volatility (e.g., if the world has more disruptions or if the company is more exposed to these disruptions, then real options such as spare capacity become more valuable). In contrast, if there were no disruptions or unexpected demand fluctuations, there would be no value to investing in optional capabilities that never get used.

[1] Interested readers can get an introduction to the subject in many books. See, for example, Richard De Neufville and Stefan Scholtes, *Flexibility in Engineering Design*, Engineering Systems Series, MIT Press De Neufville and Scholtes (2011).

2.2 Four Common Categories of Real Options for Preparation

This chapter looks at four categories of real options in which companies commonly invest in. The first is redundancy in the form of additional quantities of standard materials or assets beyond those required for normal operations. The second category is flexible productive assets, which are assets upgraded to expand the scope of their functionality (e.g., make a greater variety of products or handle a greater span of conditions). The third is emergency operations centers (EOC), which are specialized and dedicated facilities used by decision-makers to manage risk events. And the fourth category is business continuity planning (BCP), including training drills that improve the timeliness and quality of response activities. The payoff for these can be calculated from the effects of reducing the time to recovery, mitigating customer disruptions, and avoiding negative long-term consequences.

3 Redundancy

Redundant amounts of standard supply chain materials and assets such as inventory, production capacity, and multiple facilities offer an obvious option for crisis managers. Such assets require no additional expertise to create and no qualitative changes to operational processes. They only require the willingness to invest in creating and maintaining spare amounts of familiar assets, giving crisis managers the option of utilizing the extra assets to mitigate the effects of a disruption.

3.1 A First Line of Redundancy: Extra Inventory

"During the hurricane period in central America, we ensure we have more stocks in the region by applying a so-called hurricane factor in our safety stock levels," said Frank Schaapveld, senior director supply chain Europe, Middle East, and Africa (EMEA) for medical equipment maker Medtronic (Leemhorst and Crippa 2011). Extra inventory of both finished products and parts can be utilized immediately after a disruption. Even if the inventory is not sufficient to cover the entire time to recovery, it gives crisis managers breathing room to organize a response—continuing sales and operations while collecting data from suppliers, consulting with customers, and launching various recovery efforts.

All companies hold some inventory to cover both the average level of demand between regular cycles of manufacturing and shipments (cycle stock) and to handle routine fluctuations in supply and demand (safety stock). The mathematics of inventory management helps companies estimate the amount of cycle stock that balances the economics of production and transportation versus the cost of holding inventory, as well as the amount of safety stock that is needed to provide a given level of customer service in the face of uncertain demand. In addition, work-in-process inventory is the stock held while the parts or products undergo some process, such as during shipment or conversion.

At its core, inventory provides a decoupling function between links in the supply chain. The traditional view of inventory management is that cycle stock allows each stage in the supply chain—ordering, production, distribution, etc.—to operate at its own optimal rate, creating optimal order size, manufacturing batch size, and shipment size in accordance with the parameters of that activity. Safety stock allows for decoupling of smooth-running activities from random variations. Thus, for example, distribution centers hold inventory in order to decouple the manufacturing process from fluctuating customer demands; manufacturing plants hold parts' inventory to protect against variation in the inbound flow of parts. These operational safety stock sizing decisions generally assume a normal distribution of statistical variations and the ready possibility to reorder more product at any time.

In addition, companies may keep extra inventory for mitigating larger disruptions that could significantly disrupt operations. Such extra inventory also fulfills a decoupling function: isolating the company's customers from a disruption. Whether a company chooses to hold these extra inventories depends on the value at risk, the cost of holding enough inventory to cover the value at risk, the cost/possibility/timing of procuring alternate supplies in the event of a disruption, and the likelihood of a disruption.

3.2 Practical Upper Limits on Inventory

Whereas cycle stock and traditional safety stock can be modest in volume in a lean supply chain, the extra inventory to cover high-impact disruptions may be quite large and expensive if the time to recovery is long. In addition, the low frequency of large-scale disruptions means that such extra inventory will have to be carried for a long time before its value is realized, if ever. Consequently, such redundancy may be too costly in most situations. Inventories may also be bounded by perishability or hazardous materials concerns.

Inventory also increases some risks even as it mitigates others. The rationale for lean manufacturing is the avoidance of waste. In a traditional first-in-first-out make-to-stock inventory management system, defective parts arising from a defective manufacturing process may go undetected until those parts work their way through the inventory "pile" and make it into production or sale. In contrast, faster turns mean faster detection, learning, and improvement, which are keys to the concept of Kaizen (continuous improvement), which is part of the Toyota Production System. A second type of risk of waste created by inventory is obsolescence. If demand drops, the company may be stuck with too much inventory and incur costs or losses in liquidating the excess stock. Thus, although added inventory can allow a company to keep satisfying customers' demand after a disruption (at least for a time), it increases costs, introduces product quality risks, and has additional risks of overstocks. From a real options evaluation point of view, inventory adds value in the face of supply risk but subtracts value in the face of some demand risks.

3.3 Other Kinds of Redundancy

Redundancy comes in many forms. Medtronic opened a second distribution center in Europe after a risk assessment revealed that having only one distribution center posed too much risk (Leemhorst and Crippa 2011). Dual sourcing is a common supplier risk mitigation strategy. Having two suppliers with different risk profiles introduces redundancy—giving the company the option to use materials or parts from whichever supplier is not disrupted. However, in many cases additional suppliers come with additional costs because each supplier provides a smaller volume that offers less opportunity for economies of scale and amortization of fixed costs such as tooling, engineering, and contract management. Cisco considers both dual manufacturing sites as well as the qualification of alternate sites in assessing the resilience of new suppliers associated with new products (Luu 2013).

4 Flexibility

Flexibility is an asset design or specification strategy for increasing the number of potential productive uses for a given asset. This applies equally to production lines that can be configured to manufacture several products, the use of retail stores for e-commerce, or the cross-training of employees, so they can be moved between tasks, as needed. Manufacturing sites, for example, can be either specialized (one location can produce only one product from one set of parts) or flexible (each plant can produce many different products from many different sets of parts). Flexibility enables resilience. If one asset becomes disrupted, other assets can be redeployed to produce, store, or move the product handled by the disrupted asset.

As real options, flexibility and redundancy complement each other. Redundancy—in particular extra inventory—provides near-instantaneous coverage, but only for a finite duration. Flexibility provides longer-term coverage but usually requires some initial reconfiguration time. Thus, redundancy provides time for organizations to "fire up" their flexible assets by reconfiguring equipment, repurposing machinery, contacting alternate suppliers, reassigning personnel, shipping raw materials to the backup facility, and so forth. Both redundancy and flexibility are a means to reduce the gap between the moment of disruption and the beginning of recovered production, service, and supply.

4.1 Flexible Manufacturing: The Option to Make Anything

Dr. Pepper Snapple Group (DPS) built its Victorville, California, plant with flexible bottling lines that can each handle both cold- and hot-fill products, including carbonated soft drinks, energy drinks, teas, juices, and bottled water. Moreover, each line can handle different container sizes.[2] Demand volatility of the individual bottle sizes and flavors is high due to fickle consumer preferences, retailer promotions, seasonality, and weather. If each variety and size of beverage used a different bottling line, utilization of each line would also be very volatile and many lines would be idle much of the time while others ran out of capacity. The flexibility to make different products on the same equipment enables risk pooling—a reduction in overall risk or volatility by aggregating across multiple risks or volatilities.

Full flexibility—being able to make anything anywhere—is usually prohibitively expensive or infeasible due to the natural and economical specialization of machine tools and labor. Yet research shows that a company can achieve extremely high levels of overall flexibility with only modest amounts of flexibility at the plant level (Jordan and Graves 1995). The strategy requires that each plant be able to make just two different products but arranging this flexibility in a special way.

For example, imagine having four factories, A, B, C, and D and four products, 1, 2, 3, and 4. Factory A can make products 1 and 2; factory B can make products 2 and 3; factory C can make products 3 and 4; and factory D can make products 4 and 1. If factory B gets disrupted, threatening deliveries of products 2 and 3, then both factories A and C can chip into cover for the loss of factory B. Even if factory C is already running at capacity, it can still take over production of product 3 by shifting C's responsibilities for product 4 to factory D. As long as some spare capacity exists somewhere in the network, production can be shifted. By creating a "daisy chain" of product assignments to factories, the company can literally shift production around the network and create a system that is flexible enough to make every product even if one facility is disrupted.

Flexibility requires some amount of system-wide redundancy. Assuming in the example above that each of the four factories has the same capacity and that each of the four products has the same demand, then this flexibility strategy would require each factory to be able to boost production by about 33% on average to cover for the disrupted fourth factory. Yet that 33% spare emergency capacity figure enables full recovery if any of the four factories is disrupted and is far more cost-effective as an option than having duplicates of all four facilities.

[2] http://www.drpeppersnapplegroup.com/files/Beverage_Industry-DrPepper_125th_CoverStory_Victorville_Plant_Opening.pdf

4.2 Flexible Distribution Networks: Emergency Realignment

Walmart operates its distribution centers (DC) to provide this kind of flexible fail-over capacity with minimum redundancy. Each of its 150+ DCs in the USA serves about 90–100 stores within a 200-mile radius (Walmart 2018). To prepare for disruption of a DC, each DC has two or three nearby DCs that are designated as backups. If one DC goes down, an emergency realignment of the service areas of the backup DCs fills in for the disabled DC.

This flexibility requires that Walmart have some spare capacity in each DC so that it can continue to serve both its original region while also contributing to serving the region that has a disabled DC. Although a simplistic analysis would suggest that each of the two or three backup DCs would need between 33 and 50% extra capacity to cover the 100% loss of another DC, the required redundant capacity is much smaller. First, each backup DC can increase its output through overtime and extra labor. More important, the dense DC coverage means that each backup DC has its own backup DCs. Any shortage in the regions served by the first-line backup DCs can be covered by the second-line backup DCs.

4.3 Mobile Flexible Assets

Normally, cellular communications provider AT&T relies on a large network of fixed assets (cell towers, backhaul fiber optics and microwave towers, and data routing systems) to handle cellular data, voice, and texts. When Superstorm Sandy threatened the East Coast, AT&T sent in the COWs—which stands for Cell on Wheels—special truck trailers that can erect a high-capacity cellular network station anywhere, anytime. The self-contained trailers include multi-beam cell-tower antennas on a telescoping tower, network equipment, a power generator, and cooling equipment. Different types of COWs perform different functions, such as 5- and 18-beam cell towers, mobile command center, and microwave backhaul for relaying the combined traffic from the cellular signals to a distant high-capacity Internet connection (Weintraub 2013). The company also has a fleet of smaller Cell on Light Truck (COLTs) that use a satellite uplink to provide service. If a natural disaster strikes, AT&T can send in these vehicles to immediately restore cellular service while the harder job of repairing downed cell towers and power lines takes place.

Yet COWs are not just for handling disruptions during a disaster. In 2012, AT&T sent nine COWs to Indianapolis for Super Bowl XLVI to help support the massive surge in cellular use that occurs when 85,000 fans, press, staff, and players inundate the stadium and surrounding area (Smith 2012). Indeed, the company deploys COWs to sporting events, festivals, large public gatherings, or any time the company expects a surge in demand for cellphone usage.

An event like Superstorm Sandy creates both a supply disruption and a demand surge. The storm knocks out power and cell towers at the same time that call volumes increase two to four times over normal daily averages, according to Tim Harden, President, Supply Chain and Fleet Operations for AT&T Services, Inc. (Sheffi 2015). Such flexible assets serve both for causal pathways involving disruptions of operations or supply as well as pathways creating surges in demand, which accrues to the value of these real options. A given real option might have multiple deployment scenarios, implying a much higher overall probability of being used and a much higher expected payoff.

5 Places: Emergency Operations Centers

In the heart of Walmart's Bentonville, Arkansas headquarters sits a mostly empty room. At first glance, it could be a break room with a dozen tables and about 50 chairs. Tabletop placards for different Walmart groups seem to hint at assigned seating for an upcoming luncheon. Yet the people and the luncheon never seem to come. Further scrutiny suggests a more utilitarian purpose, because every spot at the table has a tangle of power cords and computer connections at the ready. On the walls, hang big-screen monitors and maps of Walmart's operations. The room is Walmart's Emergency Operations Center (EOC). In the corner, a few staffers monitor global news feeds, weather maps, earthquake reports, and the like. The EOC springs into action when a significant disruption calls for a coordinated response. Thankfully quiet most of the time, the room is there when it is needed.

Near the EOC site is Walmart's equivalent of a certified 911 emergency dispatch center. If there is a problem in a Walmart store or facility, anytime and anywhere across the nation, store employees can call this 24×7 center. The center can also detect store situations through in-store sensors and remote cameras. Whether as a result of a call from store personnel or through automatic detection, the center can dispatch security, firefighters, medical help, or whatever else is needed. The call center handles 400,000 calls a year—similar to the call volume of the Los Angeles Fire Department. The vast majority of the calls are minor: a leaky roof or a false alarm on a smoke detector. Some of the calls are more serious, but localized: a fistfight in the parking lot or somebody slipped and fell. A few make bigger headlines, such as the attempted knifepoint abduction of a toddler by a deranged person in June of 2013.[3] And some are larger-scale problems that require a more coordinated response, such as a regional power outage or a hurricane.

5.1 Facility Monitoring: Who's Minding the Stores

Associated with investments in an EOC are investments in monitoring. Walgreens, like Walmart, uses in-store sensors to monitor each of its 8,300 US locations. The

[3] http://www.cbs12.com/news/top-stories/stories/vid_8457.shtml

raw data flows to Walgreens' centralized EOC—termed a security operations center (SOC)—which handles the retailer's safety, security, and emergency response needs. "In the SOC, we monitor all the burglar and fire alarms in our stores, and, on average, three stores are robbed each day and two stores have break-ins every night," said Jim Williams, Manager, Walgreens Emergency Preparedness and Response, Asset Protection, Business Continuity Division (Sheffi 2015).

Electrical power sensors alert Walgreens to infrequent but highly consequential blackouts, which let the company quickly take steps such as contacting the power company, dispatching generators, or sending refrigerated trucks to recover perishable inventory. Walgreens' stores carry both refrigerated foods and temperature-sensitive pharmaceuticals, so faster detection means less spoilage. "The process has saved us over $3.6 million in perishable goods in just one year," Williams said (Sheffi 2015). SOCs and emergency operations centers are on the frontline of detection of disruption, especially those occurring at the company's facilities.

5.2 The Local and the Global

Whereas Walmart has one EOC for the entire company at its headquarters, Intel has an EOC at each of its large multi-billion dollar facilities located around the world. Each local Intel EOC has a satellite phone (in case all other communications links break down) and a set of key response personnel (e.g., security, HR, and Environmental Health and Safety). EOCs in earthquake regions have out-of-building capabilities (tents, portable generators, etc.). In addition to these local physical EOCs, Intel has a Corporate EOC (CEOC) that convenes virtually because Intel's executives are not all based in one location. The CEOC includes experts in engineering, procurement, manufacturing, logistics, and even public relations, and it plays a major role in larger disruptions when Intel must shift resources and activities between sites.

6 Ready for the Worst: Business Continuity Plans

General Dwight Eisenhower, Supreme Commander of Allied Forces in World War II and the 34th President of the USA, said, "In preparing for battle I have always found that plans are useless, but planning is indispensable" (Ratcliffe 2014). Business continuity planning (BCP) is a process for preparing disruption responses to accelerate the response process and reduce the probability of erroneous responses. "The collective Intel response underscores the importance of creating and sustaining a well-prepared response and recovery capability. Speed is vital," said Jackie Sturm, Intel's Vice President and General Manager of Global Sourcing and Procurement about Intel's response to the 2008 earthquake in Sichuan near Intel's Chengdu facility (Sheffi 2015). Whereas redundancy and flexibility often invest in tangible assets, BCP creates intangible assets for decision-makers in the form of knowledge and training of what to do during a disruption.

6.1 When the Going Gets Tough, the Tough Use Playbooks

Since 2008, Cisco has created 14 supply chain incident management playbooks. The playbooks—Cisco's term for BCP—cover relatively high-likelihood disruptive events. The company's attitude toward the playbooks is, "if you get caught twice, then shame on you" (Luu 2012). The playbooks vary across locations, depending on the types of disruptions typically experienced at those locations. For example, Texas has tornados, whereas Thailand has monsoons and floods. A survey found that the top contingencies covered by BCP include loss of IT (91% of organizations surveyed have plans covering that), followed by fire (68%), loss of a site (62%), employee health and safety (52%), loss of suppliers (43%), terrorist damage (37%), and pressure group protest (22%) (Jüttner 2005).

Cisco creates a new playbook by pulling together relevant elements of existing playbooks and using supply chain risk management (SCRM) analytics and know-how. After each incident, Cisco reviews its response and the responses of suppliers to collect the lessons and improve the playbook (or create a new one) for the future. After the Thai floods of 2011, for example, Cisco looked at how suppliers handled the floods (e.g., how they moved delicate test equipment to the second floor or built barriers around key buildings) and incorporated those tactics into its flood playbook.

Cisco's playbooks list the types of questions vital to answer in a crisis, such as how many suppliers are in the region, what parts or products they make, how they could be impacted, whether there are backups for the suppliers, and how to assess the actual impact on the ground. The playbooks also contain templates, checklists, and other materials to assist in managing and mitigating a disruption.

Similarly, Medtronic uses action-oriented BCP based on checklists (Raso 2010). Each checklist element includes a task, its status, the people responsible, the timing of the task, and optional supporting documents. Medtronic's planning process stresses the information, people, and actions required for recovery and continuity. The information flow elements of its BCP ensure the right people learn of the event as soon as possible via a mass notification system and that people working on continuity have the information they need to do their jobs.

The philosophy behind Medtronic's business continuity plans is to enable the company to operate at a predetermined, minimum capability/service level and meet demand during a disaster. Because Medtronic's medical device products are crucial to the health of patients, continuity of supply is essential. Each of Medtronic's plans addresses a worst-case scenario because a large disaster requires as much pre-planning as possible in order to accelerate the response. Lesser disasters can always use a subset of the plan. As imperfect as plans might be, planning helps companies think through and predetermine how they might react to disruption, who should be involved in the response effort, and what assets should be prepared ahead of time.

6.2 Playbooks to the People

The primary value of a BCP is only realized with some further investment in training. As with Cisco, Juniper Networks created a series of business continuity plans to cover disruptions linked to facilities, locations, suppliers, and geopolitical events. Steve Darendinger, vice president of worldwide procurement at Juniper Networks explained that each BCP is encoded in a PowerPoint presentation that can be pushed to employees' computers wherever they are (Sheffi 2015). The plans also fit on a USB thumb-drive for physical distribution if computer networks are not available. Juniper created online video training courses for its BCPs and by 2012 had trained about 75% of its worldwide operations staff in the use of the BCPs. Other companies, such as Medtronic, use third-party incident management software to distribute BCPs to stakeholders when they need them.

6.3 Drill, Baby, Drill

Cisco holds annual BCP drills to ensure that its plans are actionable and incorporate the lessons from past disruptions (Luu 2012). The drills simulate the chronological progress of the causal pathway with simulated news stories of the event, government responses, and public activity. As the drill progresses, participants must decide how to monitor the situation, prepare for consequences, and recover from the event. Participants' actions might include EOC activation, changes or movement of inventory, changes in production, redeployment of resources, communications with suppliers and customers, and so forth. The drill facilitators then react to each participant decision with the effects (and unintended consequences) of the decision. A postmortem of the drill helps refine the plan and train participants for future and actual crises.

For example, a 2009 drill tested Cisco's response to an influenza epidemic in China (Anupindi 2011). Although this simulated pandemic only affected China, by running the drill the SCRM team realized that it needed to examine its business in Mexico more closely, given Mexico's rising importance to the company. Cisco works with several dozen supplier and partner sites in Mexico, and some of them are in regions prone to hurricanes. The drill prompted SCRM members to discuss proactive steps they could take to ensure continuity of supply if a hurricane hit that region.

Drills such as the ones Cisco undertakes also serve to train people in crisis management: who does what, what to expect, and how to respond. Drills test the efficacy and completeness of a BCP or a playbook as well as the readiness of disaster resources. Through drills, companies sometimes uncover significant gaps in their preparedness. When one company simulated an earthquake at headquarters, most of the event went as planned except for one crucial detail. Participants discovered that a key computer server that was essential to 100% of the sales of the company had no failsafe outside of the vulnerable headquarters building. Thus, the drill enabled the company to find a gap in its risk mitigation efforts and correct it before a real emergency occurred.

Speaking after hurricane Katrina in 2005, Walmart's CEO H. Lee Scott Jr. summed up the value of all these preparations and planning—the development of options for managing disruptions. "We have an infrastructure that allows us to react," he said (Barbaro and Gillis 2005). Walmart managed to reopen 66% of its stores in the affected area within 48 hours. Within one week, 93% of stores were reopened (Opstal 2007). Walmart earned high praise for its timely and effective response. "If the American government would have responded like Walmart has responded, we wouldn't be in this crisis," said Aaron F. Broussard, president of Jefferson Parish in the New Orleans suburbs, during a tearful "Meet the Press" interview (Barbaro and Gillis 2005).

6.4 The Bigger Picture: From BCP to BCM to ERM

At Medtronic and other companies, business continuity plans are part of a larger investment in business continuity management (BCM) (Raso 2010). BCM is the overarching process of planning, disseminating, executing, and refining BCPs. In turn, BCM is a subset of enterprise risk management (ERM). BCM tends to focus only on operational risks such as disrupted supply, production, distribution, and service. ERM, in contrast, considers operational risks plus many other risks such as financial risks, regulatory risks, competition, customer disruptions, talent risks, product quality, intellectual property risks, compliance risks, corporate social responsibility risks, and others.

7 SCRM as a Real Option

Many companies see risk management as just another cost with no sure benefit. In the words of a transport manager, "It takes resources away from what our core business is" (BASF 2012). An unused EOC seems like squandered office space and corporate resources. BCP and drills take time away from day-to-day operations. Extra inventory is expensive and at odds with the cost-cutting mantra of lean operations. The perception of waste can seem doubly true with prevention strategies, because they intentionally seek to ensure that nothing ever happens. Yet the real option framework shows how investments in SCRM can provide value, directly and indirectly, as well as support growth.

For example, Cisco created a database of risk mitigation efforts and subsequent disruptive events. In addition to helping the company track its risk mitigation efforts, the databases let Cisco tally the direct value of those efforts (Harrington and O'Connor 2009). By documenting the improvement in recovery time resulting from its risk management processes, Cisco tracks impacts that it avoided, such as lost revenues, late shipments, and other critical business metrics.

7.1 Response Investments

Organizations such as AT&T, Cisco, Intel, UPS, and Walmart invest in response assets and procedures because they serve customers everywhere, including locations with high likelihoods of disruptions from hurricanes, snowstorms, and other natural disasters. Many multinational companies have facilities and suppliers around the globe in vulnerable areas. While the likelihood that a particular disruption will strike a particular location at a particular time is very small, the likelihood that *some crisis* will happen *some place* at *some time* is significant. Whereas the value of many real options for supply chain risks such as a specific product's extra inventory or a specific BCP is only realized if a specific category of risk event occurs, the value of ERM is realized with any type of volatility in supply, internal operations, or demand.

If and when disruptions occur, preparations for response repay in terms of both accelerated recovery and mitigated impacts. To the extent that emergency response and business recovery teams are active immediately after a disruption hits, recovery can begin immediately, shortening the duration of the disruption. Pre-organized teams, pre-created plans, a pre-configured "war-room," and pre-stocked recovery supply all help accelerate response. For example, a robust EOC and drilled recovery process helped Walmart reopen its stores faster and at lower cost than before (Cooper 2013).

"Risk management (RM) has the capacity to straddle all sides of a business. At the end of the day, it's the whole package that works in selling your product or service," said Bob Ritchie (Zurich 2011b). A key part of that whole package is the portfolio of real options that companies create for themselves and can then exercise as needed to ensure continuity of their products and services.

References

Anupindi, R. (2011). *Supply Chain Risk Management at Cisco: Response to H1N1*, case 1-428-881 March 7, 2011.

Barbaro, M., & Gillis, J. (2005). Walmart at forefront of hurricane relief. *The Washington Post*, *6*.

BASF (2012). *Responsible care management system.* http://report.basf.com/2012/en/managementsanalysis/responsibilityalongthevaluechain/responsiblecare.html.

Cooper, M. (2013). (Senior Director, Emergency Management, Walmart), *Personal Communications, 25*.

De Neufville, R., & Scholtes, S. (2011). *Flexibility in engineering design, engineering systems series*. Cambridge: MIT Press.

Harrington, K., & O'Connor, J. (2009). How cisco succeeds. *Supply Chain Management Review, July/August, 2009,* 10–17.

Jordan, W., & Graves, S. (1995). Principles on the Benefits of Manufacturing Process Flexibility. *Management Science, 41*(4), 577–594.

Jüttner, U. (2005). Supply chain risk management: Understanding the business requirements from a practitioner perspective. *The International Journal of Logistics Management, 16*(1), 120–141.

Leemhorst, L., & Crippa, R. (2011). Do or die: Manage or ignore supply chain risk? *Supply Chain Movement, 3*(Q4), 11–16. https://www.supplychainmovement.com/wp-content/uploads/Supply-Chain-Movement-Quarterly-No3-2011.pdf.

Linton, T. (2012). (Chief Procurement Officer, FLEX) *Personal Communication*, *30*.

Luu, N. (2012). The cisco method presentation at advancing supply chain risk management: Emerging challenges and strategies. In *MIT Center for Transportation and Logistics Conference*, Cambridge, MA, 10 October 2012.

Luu, N. (2013). (Senior Manager, Supply Chain Risk Management, Cisco), *Personal Communications.*

Raso, T. (2010). Focusing and measuring your continuity efforts to improve resiliency. In *Continuity Insights 2010 Management Conference*, 12–14 April 2010.

Ratcliffe, S. (2014). *Oxford essential quotations*. Oxford: Oxford University Press.

Ritchie, B., & Clare Brindley, C. (2007). Supply chain risk management and performance: A guiding framework for future development. *International Journal of Operations and Production Management, 27*(3), 303–322.

Sheffi, Y. (2005). *The resilient enterprise: Overcoming vulnerability for competitive advantage*. Cambridge, MA: MIT Press.

Sheffi, Y. (2015). *The power of resilience: How the best companies manage the unexpected*. Cambridge, MA: MIT Press.

Smith, J. (2012) AT&T Brings 9 COWs to Indianapolis for super bowl 46 (Video). *GottaBeMobile*.

Trigeorgis, L. (1995). *Real options*. Cambridge, MA: MIT Press.

van Opstal, D. (2007). Transform. *The resilient economy: Integrating competitiveness and security*. Council on Competitiveness, July 2007. http://www.nyu.edu/intercep/research/pubs/annotated-business-case_20-aug-2007.pdf.

Walmart (2018). *Our Business*, https://corporate.walmart.com/our-story/our-business. Accessed 27 Feb 2018.

Weintraub, J. (2013). Inside AT&T's 83 GB/hour mobile cell tower … or why your iPhone no longer drops out at huge events 9TO5Mac, May 19, 2013 https://9to5mac.com/guides/network-performance/.

Zurich (2011a). Measuring risk is key to protecting your business. *Insights Supply Chain Risk* (2011), 11–13.

Zurich (2011b). Taking measures to cope with delivery disruption. *Insights Supply Chain Risk* (2011), 14–16.

Chapter 10
The Future of Resilient Supply Chains

Mattia Donadoni, Sinéad Roden, Kirstin Scholten, Mark Stevenson, Federico Caniato, Dirk Pieter van Donk and Andreas Wieland

1 Introduction

Dynamism coupled with market instability continues to expose supply chains to disruptive events. The occurrence of disruptions cannot only be traced back to the multi-tiered and global nature of many supply chain configurations (Christopher and Peck 2004a; Jüttner and Maklan 2011; Sheffi and Rice 2005), but also to their interconnectivity (Knemeyer et al. 2009; Bakshi and Kleindorfer 2009). As a result, supply chain disruptions are inevitable events and a key contemporary challenge concerning how organisations and supply chains can bounce back while ensuring sustained performance outcomes (Ponomarov and Holcomb 2009). In other words, how they can improve their ability to handle disruption, thereby creating and developing a resilient supply chain.

The resilience of organisations and their supply chains has become a focal point of interest for practitioners and academics alike over the past 10 years (for a review, see Tukamuhabwa et al. 2015). This interest has been sparked by the severe impact that disruptions can have at the firm level and beyond, in terms of both short and longer term operational and financial performance (Hendricks and Singhal 2005).

M. Donadoni (✉) · F. Caniato
Politecnico di Milano, Milan, Italy
e-mail: mattia.donadoni@polimi.it

S. Roden
Trinity Business School, Trinity College Dublin, Dublin, Ireland

K. Scholten · D. P. van Donk
University of Groningen, Groningen, The Netherlands

M. Stevenson
Lancaster University, Lancaster, UK

A. Wieland
Copenhagen Business School, Frederiksberg, Denmark

G. A. Zsidisin and M. Henke (eds.), *Revisiting Supply Chain Risk*, Springer Series in Supply Chain Management 7, https://doi.org/10.1007/978-3-030-03813-7_10

Considerable attention in the literature has been given to a number of devastating examples in the last decade (e.g. the financial crises (Jüttner and Maklan 2011); the Tōhoku earthquake and tsunami and Hurricane Sandy) which highlight how disruptions that occur at one node cascade through the network. As such, the evolving empirical literature has made steady progress in measuring “disruptive events” and operationalising resilience. At the same time, less attention has been given to what “keeps managers awake at night”—what the things are that they are most concerned about. In particular, there is little knowledge about what they consider as a disruption in day-to-day management of their supply chain, what they perceive as *resilience* and how to measure it. We are also not clear on whether the definitions and measurement of resilience depend on industry context, specific organisational capabilities or supply chain strategies they employ. Against this backdrop, we aim to disentangle the concept of supply chain resilience (SCRES) and understand how it is interpreted in practice.

A two-stage empirical study has been conducted. The first stage was performed with academic experts in the field of SCRES to identify key disruptions, strategies, resilience metrics and industries where resilience is expected to be a key concern. This stage helped to set the scope of the research and identify target respondents for the following stage. Hence, based on the responses of the first stage, we involved practitioners from three industries: automotive, electronics and food, to capture what it means to be resilient in a practical context in the second stage. Their insights allow us to theorise about three aspects related to disruptions in and resilience of global supply chains:

- the nature and characteristics of key disruptions
- the features that make an industry or supply chain vulnerable or prone to disruption;
- the features of the primary strategies employed to avoid or minimise the effects of a disruption and “bounce back”.

The remainder of this chapter is organised as follows. In Sect. 2, we develop our lines of enquiry using SCRES literature. Section 3 describes the methodology adopted, with the results from stages 1 (academic experts) and 2 (practitioner experts) presented in Sect. 3, followed by a discussion in Sect. 4. The chapter concludes in Sect. 5, which includes avenues for future research on SCRES.

2 Theoretical Background

Disruptions are defined as “unplanned and unexpected events that interrupt the flow of materials and products within a supply chain” (Hendricks and Singhal 2005). A wide variety of events can potentially cause a disruption including unavailable raw materials, late deliveries, natural disasters, tainted ingredients , government regulations, machine breakdowns and cyber threats (Business Continuity Institute 2016). Clearly, this set of disruptions is hierarchical and inter-related; for example, a natural disaster could affect the availability of raw materials and the on-time performance of deliveries. As such, disruptions can have different degrees of severity (Craighead et al. 2007) and consequences (e.g. operational and financial), both within and across organisations (Bode et al. 2011; Craighead et al. 2007) that can compromise not only the ability to manufacture products but also to fulfil market requirements. While research has classified disruptions according to their impact [high, medium or low impact, e.g. Norrman and Jansson (2004) and Tang (2006)] to derive appropriate risk management strategies, others have approached the evaluation of disruptions according to the probability of occurrence and the relative magnitude (Ellis et al. 2010). Other classifications may, however, be appropriate; for example, it may be important to treat disruptions according to their origin or duration. Therefore, our first research question aims to understand the characteristics of disruptions as a starting point for determining how to treat them in future:

RQ1: What are the characteristics of supply chain disruptions that decision-makers work to actively avoid?

The severity of the disruption is affected by the portfolio of resources that companies possess. Indeed, the mitigation capacity of companies is strictly related to resources that can be deployed to reduce the initial impact and overcome the supply chain disruption. According to Sheffi and Rice (2005), companies that can shape their resources towards the development of an effective strategy for dealing with disruptions can improve their resilience. With this in mind, the SCRES literature has highlighted various strategies for dealing with disruptions in supply chains and enhancing resilience (Pettit et al. 2010; Tukamuhabwa et al. 2015). Given this, the majority of the works remain mostly conceptual, leaving a sense of ambiguity on how resilience can be fostered within organisations and in their relative supply chains, as described below.

One of the first studies on resilience in supply chains was conducted by Rice and Caniato (2003) who described two main strategies for achieving resilience—having redundancy to quickly deploy extra resources in case of emergency and being flexible to adapt to fluctuations in the business environment. Similarly, Wieland and Wallenburg (2013) argue that the resilience of a supply chain relates to a proactive ("robustness") and a reactive strategy ("agility"), the former often being built on redundancy, the latter on flexible adaptation. Christopher and Peck (2004a, b) proposed four system level strategies: re-engineer the supply chain; collaborate with other entities; improve agility; and create a supply chain risk management culture. Other studies have elaborated on formative elements such as flexibility, velocity, visibility and collaboration (Jüttner and Maklan 2011), or the human resources (e.g. training or education) as main facilitators of resilience (Blackhurst et al. 2011). Furthermore, some authors distinguish between intra- and inter-organisational antecedents of resilience (Durach et al. 2015).

Although these earlier academic studies have made progress in disentangling the concept of SCRES and identifying how resilience can be fostered, empirical understanding and support of which activities, routines, and strategies are actually adopted by managers remains underdeveloped. It is also uncertain how the strategies employed in practice compare, e.g. whether they have similar features or characteristics, which could allow for a more general contribution to understanding how resilience can be developed. Therefore, our second research question asks:

RQ2: What are the activities and strategies that organisations use to mitigate disruptions and bounce back?

So far, the SCRES literature has focused on identifying the strategies that companies can apply to make the whole supply chain resilient, but there is a lack of understanding whether the business environment in which companies operate influences the portfolio of strategies embraced by firms. To this regard, it has been suggested that determining appropriate practices for dealing with disruptions can be context-specific (Christopher and Peck 2004b). Contextual problems that plague one industry can drive the approaches adopted to build resilience by companies towards a specific set of strategies; and the context could also influence the behaviour of managers when they are faced with a disruption. So far it is unclear if, and if so, how, the characteristics of an industry relate to resilience and disruption. Taking industry features (e.g. product life cycles, supply chain characteristics, technology ratios, power structure) into consideration may help to shed light on how they shape the boundaries and capabilities through which companies build resilience. Indeed, industry characteristics might impact the frequency, magnitude and duration of disruptive effects. Hence, some industry types may be perceived to be more prone to disruption than others. Therefore, the third research question is:

RQ3: What are the characteristics of industries that make them more or less prone to a disruption?

Even within an industry sector, there are differences between organisations regarding how they manage disruptions and develop their "resilience". The well-known case of Nokia versus Ericsson, for example, demonstrates that some organisations are more resilient than others (Norrman and Jansson 2004). So far, however, we only know how resilient a supply chain is when it is too late; i.e. after it has faced a disruption when we can reflect on the impact of the event; and the academic literature offers only limited insight into this issue. There is a lack of understanding of how resilience is currently measured or assessed by organisations across sectors. According to Barroso et al. (2015), the question of "how to assess the supply chain resilience" remains unanswered.

To date, the closest metric for evaluating resilience relies on the concept of the "resilience triangle", which captures the loss in performance after a disruption has occurred (Tierney and Bruneau 2007). The magnitude of a disruption influences the depth of the triangle, while the recovery time affects the length of the triangle. The approach allows for understanding the resilience level of companies after a disruptive event has occurred—evaluating the size of the disruption and the recovery—but it is not able to evaluate (potential) resilience proactively. Moreover, it is not clear how to evaluate the impact of the various strategies that companies implement to enhance resilience. Being able to estimate the current resilience value of each entity within a supply chain in advance of a disruption would help managers to justify investments in areas that attenuate the negative and unpredictable effects of disruptions. Further, being able to quantify the level of resilience would allow stakeholders to identify the weakest node in the supply chain, invest resources and deploy strategies in an efficient way to improve the overall level of resilience. Therefore, the final research question is:

RQ4: How can supply chain resilience be measured by organisations?

3 Research Methodology

This work follows a qualitative approach in our data gathering, relying on statements and answers of two panels of experts in the field of SCRES: academics and managers. In line with the aim of this research, engaging experts on resilience helps in exploring different points of view on a phenomenon as complex as resilience. Our study comprises the following two stages in order to both captures some of the existing knowledge among academics as well as get a more detailed and nuanced view on managers' insights:

- Stage 1: Data is used from a panel of academic experts who are active in the field of SCRES.
- Stage 2: Data is used from a panel of practitioner experts from industries identified as being particularly prone to disruption by the academic experts (automotive, electronics, and food).

3.1 Data Collection and Analysis

Stage 1: Involving Academic Experts
We targeted academic experts who have contributed to the supply chain resilience literature in the past 10 years. A total of 36 academic experts were sent an invitation letter outlining the conceptual background and purpose of the study. Given the exploratory nature of this stage, the questionnaire was based on open-ended questions regarding: (1) key disruptions; (2) resilience strategies; (3) industry risk levels; and, (4) metrics for measuring resilience in line with the four research questions of this study. Responses were received from 23 of the academic experts contacted, i.e. a response rate of 64% (Table 1). From the original list of responses, we eliminated those that did not provide any valuable insights (e.g. respondents who were not able to provide any metrics to calculate resilience) or we merged similar answers for having distinguished and concise options (e.g. respondents who stated "quality-related

Table 1 Descriptive information about respondents in the study (Stage 1)

Country	N	%
UK	8	35
USA	5	22
Italy	2	9
Germany	2	9
Switzerland	1	4
Japan	1	4
Denmark	1	4
Portugal	1	4
Netherlands	2	9
Total	23	100

problems" with others like "parts quality" by creating one single label like "quality incident"). The main goal at this stage was to obtain a list of potential responses to be used for structuring the questionnaire for the second stage of the study and for selecting the right target practitioners.

Stage 2: Involving Practitioner Experts

The objective of this second round was to obtain a ranking classification around the most feared disruptions, deployed strategies for handling disruptions, and how resilience is actually measured by organisations. In this regard, the results from Stage 1 enabled a more structured questionnaire design for Stage 2: from the original list of disruptions (question 1) and resilience strategies (question 2) generated, the seven highest ranking options and for the measurement of resilience (question 4) the four highest ranking options were identified. We developed a seven-point scale for practitioners to evaluate the importance of each item (e.g. with (1) "most important threat" to (7) "least important threat"). Furthermore, we selected the three highest scoring industries in terms of risk (question 3) for practitioner respondent selection, i.e. automotive, electronics and food.

90 practitioners across Europe that were considered to be specialists in the area of SCRES, or knowledgeable of their organisation's supply chain risk management strategy, were contacted. Responses from 43 practitioners (response rate of 48%) were received. Additionally, respondents were also asked to comment upon their choice of answers so as to provide further context and background. Table 2 provides descriptive statistics on the respondents. The majority of companies involved in this stage are food companies (63%), followed by electronics companies (21%) and automotive companies (16%).

Table 2 Descriptive information about respondents in the study (Stage 2)

	N	%
Company employees		
1–200	7	16
201–500	2	5
501–1000	1	2
1001–5000	3	7
5001–10000	3	7
10001–25000	6	14
25000+	21	49
Total	43	100
Industry		
Food	27	63
Electronics	9	21
Automotive	7	16
Total	43	100
Country		
Germany	4	9
Netherlands	19	44
Spain	1	2
Sweden	1	2
Turkey	1	2
UK	5	12
USA	1	2
Italy	10	23
Switzerland	1	2
Total	43	100

4 Results and Discussion

4.1 Insights from the Academic Panel

4.1.1 Key Disruptions that Decision-Makers Actively Work to Avoid or Eliminate

The data from the academics on key disruptions were classified to obtain a clearer picture of the items listed. The original list of disruptions was quite heterogeneous regarding the nature of the problems and contained different answers. Indeed, we obtained rich information regarding key disruptions, but in turn, some answers were at a different level of categorisation. For instance, some respondents provided precise disruptions (e.g. earthquakes, flood, quality-related problems or counterfeiting) while others just listed some classification like “operational disruptions” or “everyday dis-

Table 3 Relevance of supply chain disruptions according to the academic experts

Supply chain disruptions	Respondents (%)
Network issue	73
Insolvency in the supply chain	40
Demand-side issue	33
Quality incident	27
Natural disaster	27
Unplanned IT or telecom outages	20
Machine breakdown	20
Counterfeiting	13
Strike	13
Act of terrorism	13
Fire	13
Business ethics incident	13
New laws, regulations	13
Currency exchange	13
Cyber attack	7
Civil conflict, political uncertainty	7
Intellectual property violation	7
Health and safety incidents	7

ruptions". So, initially, we grouped those options by classifying them according to the Tang (2006) framework for distinguishing them between operational (small to medium impact) and disruption risks (high impact). Then, we enlarged the nomenclature by looking for well-known risks (e.g. unplanned IT or telecom outages, adverse weather, strikes and currency exchange rate volatility) (Business Continuity Institute 2016). Such procedures helped in having a list of unique elements both "operational" and "high-profile" events. The results are shown in Table 3 listed according to the percentage of respondents referring to a particular type of disruption.

Concerning the first research question (RQ 1), when we consider Table 3, we can see that academics are more concerned with large-scale, high-profile disruptions related to network disasters, insolvency in the supply chain and demand-side issues (such as demand forecasting, loss of customers or problems in complying with customer's requirements). These types of disruptions align with recent conceptualisations of supply chains as networks and embrace both physical and support supply chains (Carter et al. 2015). The SCRES literature is grounded in the notion that resilience should be designed into supply chains as a primary feature for responding to unforeseeable and extreme events.

4.1.2 Strategies Employed to Enable Organisations to Cope with Disruptions

Academic respondents were also asked to identify strategies that may be employed to mitigate the harmful effects of disruptions. Indeed, to address the second research question (RQ 2), an overview of strategies for fostering resilience was sought. The data on key resilient strategies were classified based on previous categorisations (Pettit et al. 2010; Tukamuhabwa et al. 2015) to obtain a clearer picture of the items listed. Accordingly, we grouped similar responses under the same strategy to make them comparable. For example, in line with SCRES literature (Tukamuhabwa et al. 2015; Hohenstein et al. 2015) we grouped answers such as postponement or modular product designs under the heading of flexibility. These strategies are shown in Table 4.

Eighteen heterogeneous strategies were highlighted by the respondents, with redundancy (e.g. having additional inventory, capacity or suppliers to allow a company to promptly cope with and overcome a disruptive event), overwhelmingly selected as the key strategy for enhancing resilience.

Additional capacity, stock or suppliers are resources that can be immediately used during a disruption. Business continuity plans are cited also as an important resilience mechanism. Perhaps unsurprisingly, managers tend to rely mainly on flexibility coupled with a set of other strategies. Flexibility is defined as “the ability to react or

Table 4 Resilience strategies identified by the academic experts

Resilience strategies	Respondents (%)
Redundancy	83
Business continuity planning	43
Flexibility	39
Collaboration	39
Supply chain design	30
Visibility	13
Insurance	13
Building security	9
Contracts	4
Safety rules	4
Training competitors	4
Emergency centre	4
Hedging for commodity price risk	4
Resilience software	4
Quality practices	4
Financial solutions	4
Risk management practices	4
Supplier evaluation	4

transform with minimum penalties in time, cost, and performance" (Upton 1997). Building on this, practitioners deploy strategies that help them to quickly reconfigure activities for matching changes in their business environment. Strategies which are not strictly designed for creating resilience (e.g. collaboration, supply chain design) are deployed on a daily basis mainly for cost efficiency goals, but in turn, help companies in dealing with a different spectrum of risks. Practices such as information sharing with customers and suppliers, long-term agreements, and customers and suppliers' co-development are all practices that can enhance a collaborative approach within supply chains (Handfield and Bechtel 2002; Spekman 1988). Looking at such strategies, it is worthwhile emphasising their variety: ranging from close relationships with upstream/downstream partners (e.g. creating a collaborative approach to share information) to internally focused organisational effort (e.g. building safety stock).

4.1.3 Industries Perceived to Be the Most Prone to Disruption

The third research question (RQ 3) examines the impact of industry on resilience. Specifically, respondents were asked to list the industries they anticipated as being particularly prone to disruption. The results are presented in Table 5 where the top three industries are automotive, electronics and food. While it has been acknowledged that organisational resilience strategies can be influenced by the nature of business and industry in which the business resides (Christopher and Peck 2004a), the SCRES literature provides few insights on this. Our study helps to better understand this claim. Specifically, automotive and electronics industries are complex and global, in which numerous entities are involved (e.g. a multitude of tiers) as the products are built using a large number of heterogeneous parts. Such inherent factors contribute to exposing automotive and electronics companies to a higher level of complexity and

Table 5 Industries perceived to be the most prone to disruption by the academic experts

Industries	Respondents (%)
Automotive	60
Electronics	33
Food	33
High tech	20
Fashion	20
Aerospace	20
IT	13
Pharmaceutical	13
Chemical	7
Banking	7
Retailing	7
Logistics	7

ultimately, vulnerability. Moreover, given the complexity of these supply chains, it is difficult to closely monitor these chains for potential disruptions since companies lack visibility of their supply chains. Results also suggested that the food industry is vulnerable to disruption. In particular, academics referred to the effects of specific risks that are part of the context that can increase the level of vulnerability. One academic stated: "the process industry and particularly the food industry is prone to disruptions as operations take place 24/7 and perishability adds another dimension to managing disruptions." Given that food products may have perishability constraints, may be based on raw materials with volatile demand and supply markets and/or prone to contamination (2013 EU horse meat scandal) and food safety concerns, this result is perhaps not a surprise.

4.1.4 Metrics for Assessing Supply Chain Resilience

Finally, the last research question (RQ 4) aimed to identify common approaches to the measurement of resilience. Thus, academic experts were asked to list the key metrics for evaluating resilience. This remains an unresolved issue in the literature, reflected in the diversity of answers that range from metrics such as the recovery time to general performance frameworks such as SCOR. Hence, while our results in Table 6 include some clear metrics that can be used to measure resilience, other responses cannot be directly used to measure the level of resilience. We, therefore, assume that this question was rather difficult to answer for the academic experts.

The most commonly cited metric is recovery time. Almost all respondents agreed with the idea of calculating the interval in time between the occurrence of a disruption and full recovery. Although the recovery time is commonly used in the literature as

Table 6 List of resilience metrics

Metrics	Respondent (%)
Recovery time	73
Recovery cost	20
Market share (before and after disruption)	20
Contingency strategies cost	13
supply chain resilience Assessment and management (SCRAM)	13
Customer service	7
Suppliers' dependency (first tier, second tier)	7
Time to survive	7
supply chain risk management maturity model	7
Value at risk	7
Supply chain operations reference model (SCOR)	7

a proxy for estimating resilience, it can typically only be evaluated after a disruption has occurred and hence does not help in measuring the level of resilience of a supply chain or organisation in advance.

This also applies to the second most referred to metric, i.e. recovery cost, which entails the total cost incurred by the company to recover from disruptions. Similarly, the contingency strategy cost which expresses the total cost needed for implementing such strategies required for counteracting the detrimental effects of disruptive events. More generally, the measures can be grouped into cost-related factors and time-related ones, while another distinction is between—uninterrupted—performance measures and preventative ones.

4.2 Insights from the Practitioner Panel

4.2.1 Key Disruptions that Decision-Makers Actively Work to Avoid or Eliminate

In answering the first research question, practitioners were asked to score the seven most frequently referred to disruptions from Stage 1, in terms of relevance to their organisation (on a seven-point scale with 1 being the most important threat and 7 the least important threat). Results are presented in Fig. 1. The most feared disruption according to the practitioners is a quality incident arising from product and/or service issues. Indeed, quality problems can compromise the ability to fulfil market requirements and guarantee the sustainability of the business. For instance, one of the participants stated that "*focus on quality is key for long-term performance*". Besides, quality issues can also potentially impact how consumers perceive the image as "*managing quality problems help them avoid reputational damage*".

The second most feared disruption is caused by demand risk, followed by network risk. The former entails demand fluctuations, the entry of new competitors, and changes in customer requirements; and the latter is related to upstream and downstream flows. Network risk includes all problems arising from a network perspective, which includes the physical and support supply chains (Carter et al. 2015). The global nature of today's supply chains can be a key issue for managing business efficiently as for example when companies "*import products from different countries into Europe, we have to work with transport delays which lead to production delays*". In the middle of the ranking, practitioners positioned disruptions like supplier insolvency and machine breakdowns. The least relevant disruption is a natural disaster. This is an interesting result considering that the origins of supply chain resilience literature lie in the analysis of low probability and high-impact events but, according to our findings, practitioners seem to pay little attention to natural disasters. In this regard, the supply chain disruption characteristics which drive the decision-makers are the tangibility of such problems which shape their behaviour and helps them in perceiving the potential detrimental effects immediately (e.g. quality problems).

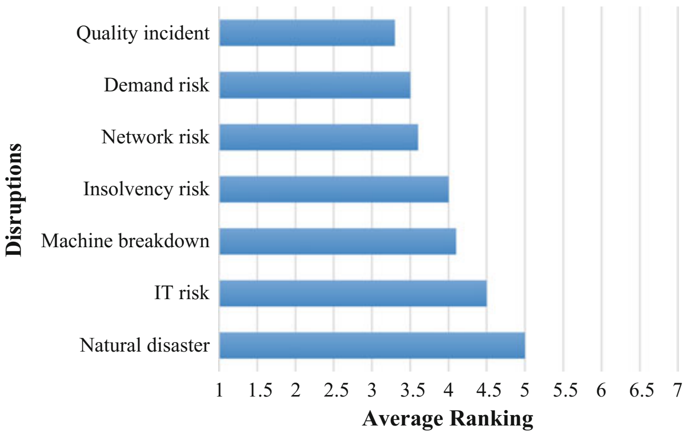


Fig. 1 Disruptions feared by the respondents (from "1" most to "7" least feared)

Besides, even though high-impact events attract the attention of scholars and affect companies severely, practitioners still tend to ignore them.

4.2.2 Strategies Employed to Enable Organisations to Cope with Disruptions

Practitioners were asked to rate the seven most frequently referred to supply chain strategies from stage 1 for coping with disruptions (on a seven-point scale with 1 the most commonly employed strategy and 7 the least commonly strategy employed). Such list derived from stage 1 helped in linking findings to the second research question. Figure 2 depicts that flexibility is the leading strategy applied by managers for overcoming the detrimental effects of a disruption. Flexibility can improve the ability to adapt operations to face up to a misalignment in the environment quickly. For instance, one of the practitioners explained: "*when we face disruptions, our type of approach is production anticipation or postponement to fulfil our customers' orders.*"

According to the results, practitioners tend to rely on supply chain design, embedding redundancy (e.g. additional capacity, extra stock) and collaborating upstream and downstream in the chain with almost the same level of importance. The importance attached to these strategies aligns with the SCRES literature. Supply chain design is a proactive strategy that allows a manager to switch from one option (e.g. a supplier) to another if needed. Redundancy is typically associated with resilience because it is a straightforward but at the same time very expensive strategy (Tukamuhabwa et al. 2015) that a company can chose to apply as a first response to disruptions. Collaboration upstream and downstream embraces the ability to work jointly towards a common goal where, in the case of a disruption, there is a reduction

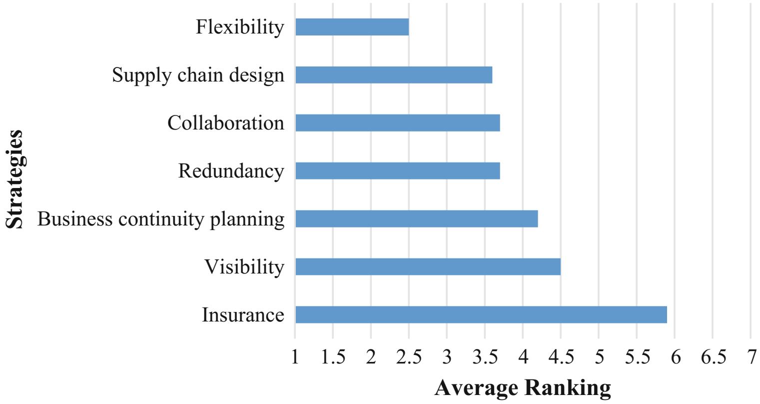


Fig. 2 Strategies employed to cope with disruptions (from "1" most to "7" least commonly employed)

of resources and efforts are required to monitor the disruption and put in place a mitigation and recovery strategy. Practitioners then referred to business continuity planning and visibility. To a certain degree, this is a surprising result since visibility is one of the most quoted strategies in the SCRES literature. The least deployed strategy is insurance, which is associated with the ability to cover financial losses; but it is not able to guarantee continuity in case of operations problems and can only partially cover the detrimental consequences of disruptions. It suggests that our respondents tend to think more in terms of customers' satisfaction than in terms of money lost.

4.2.3 Metrics for Assessing Supply Chain Resilience

Practitioners were asked to rate four metrics from Stage 1 for evaluating the level of resilience (on a four-point scale with 1 being the most important measurement and 4 the least important measurement). Due to the diversity of answers, we opted for a four-point scale, as we used the clear metrics proposed that can be used to measure resilience. Thus, we dropped those answers that cannot be directly used to measure the level of resilience (e.g. SCOR). Figure 3 shows the results, which helped us to cover the last research question (RQ 4).

The recovery time appears to be the main measure for capturing the level of resilience. Following a disruption, a company can estimate its resilience level by calculating the time taken to return to normal operating performance. Practitioners ranked the recovery cost as the second most important measurement, which refers to the sum of costs accrued following disruption recovery activities. The third most important measurement is the contingency strategy cost, which is based on an evaluation of the economic impact of deploying resilience strategies. According to practitioners, the least important measurement is market share.

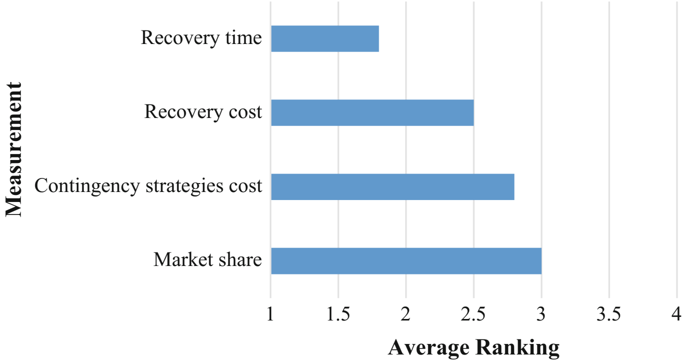


Fig. 3 Measurement of supply chain resilience (from "1" most to "4" least important measurement)

5 Conclusion and Future Directions

We contend that resilience is one of the most prominent and, at the same time, difficult research streams related to SCRES. Defining disruptions, and then understanding the level of resilience required, is crucial for improving the overall resilience capabilities in supply chains. The main aim of this work has been to investigate what managers understand as disruptions and resilience and how they measure these constructs. Our design has enabled us to explore the converging and diverging views from academics and managers.

The first research question (RQ 1) aimed to identify the characteristics of supply chain disruptions that decision-makers work actively towards avoiding. In relation to what is a disruption, there are clear commonalities between what practitioners and managers perceive to be disruptive events, coalescing around network-based events, demand side risk and quality risks. To categorise these, it could be argued that practitioners focus on operational risks or challenges that occur on a daily basis (low impact, high probability) rather than focussing on potentially higher impact disruptions with wider spread consequences (high impact, low probability). Arguably, once they have built a resilient approach towards these highly probable events, they will have the resources available to face up to more low probability, high-impact disruptions as argued in the SCRES literature. To address the second research question (RQ 2), we asked respondents to provide (academics) or to rank (practitioners) strategies that can be deployed for enhancing resilience. The use of flexibility, supply chain design and supply chain collaboration feature across both pools of respondents when referring to resilience strategies employed. Such findings are aligned with previous works on SCRES (Rice and Caniato 2003; Christopher and Peck 2004a, b; Jüttner and Maklan 2011).

Concerning the third research question (RQ 3), we deepened the analysis in emphasising whether the industry can play a role in defining how resilience is pursued by companies. To this extent, we asked academics to list industries where resilience is considered to be a key concern. We found how complex and global industries, like automotive and electronics, are considered to be more disruption prone. The food industry was chosen for its specific risks like perishability constraints, volatile demand and supply markets.

Lastly, the fourth research question (RQ 4) sought to capture the metrics considered important for measuring resilience. The debate around this question continues in the literature. Our results suggest an agreement between academics and practitioners on how resilience can be measured. Traditional risk management has focused on evaluating the probability and impact of a risk, whereas both types of respondents refer to the recovery time as the main measurement for assessing resilience. This finding reports applications in the automotive industry, among others, as a distinction between time-to-recovery (TTR) and time-to-survive (TTS) (Simchi-Levi 2015). This, however, seems an inadequate measure for proactively enhancing the resilience of a supply chain, and the results show how this area is still far from being understood. While our research aimed at providing more insights into the nature of disruptions and resilience, it also helps in providing future avenues for research on SCRES in the supply chain management discipline.

First, as we focused on three specific industries in the second stage of the study, further research is needed in order to understand how automotive, electronics and food companies generate resilience. That means understanding whether there are practices that are constrained by the application context or there are cross-industry practices going beyond the boundaries of the industry.

Second, as pointed out by Tukamuhabwa et al. (2015), considering the ability of companies to overcome disruptions without embracing cost analysis is an incomplete view. Indeed, companies should be able to bounce back from disruptions in a cost-effective way (Hamel and Välikangas 2003; Yao and Meurier 2012). Further research should evaluate how the economic sphere shapes the portfolio of practices that managers adopt for enhancing resilience. In fact, this constraint can potentially lead to a sub-optimal solution.

Third, there is a need to focus on quantifying the level of resilience. As shown by Kamalahmadi and Parast (2016), even if SCRES has become a relevant topic, few studies have tried to propose resilience measures. To this extent, managers can be reluctant to invest resources in strategies for enhancing resilience if they are not able to prove the return or benefits that they will obtain in the long term. The focus on flexibility and time-to-recovery can be interpreted as an indicator of the problems currently faced in this respect. Indeed, creating resilience means improving the ability to proactively prepare for potential disruption and immediately respond by having, for instance, additional resources (Wieland and Wallenburg 2013). Furthermore, considering the highly inter-connected nature of companies in today's global landscape, SCRES is determined by the weakest node in the chain. To this extent, previous studies have shown how the concept of resilience is complex and permeates beyond the boundaries of a single company (Craighead et al. 2007; Wakolbinger and Cruz 2011). As we develop our understanding of this phenomenon, we must, therefore, seek to advance our approach to analysing it.

References

Bakshi, N., & Kleindorfer, P. (2009). Co-opetition and investment for supply-chain resilience. *Production and Operations Management, 18*(6), 583–603.

Barroso, A. P., Machado, V. H., Carvalho, H., & Cruz Machado, V. (2015). Quantifying the supply chain resilience. In H. Tozan & A. Ertürk (Eds.), *Applications of contemporary management approaches in supply chains* (pp. 13–36). London: InTech.

Blackhurst, J., Dunn, K. S., & Craighead, C. W. (2011). An empirically derived framework of global supply resiliency. *Journal of Business Logistics, 32*(4), 374–391.

Bode, C., Wagner, S. M., Petersen, K. J., & Ellram, L. M. (2011). Understanding responses to supply chain disruptions: Insights from information processing and resource dependence perspectives. *Academy of Management Journal, 54*(July), 833–856.

Business Continuity Institute. (2016). *Supply chain resilience report 2016*.

Carter, C. R., Rogers, D. S., & Choi, T. Y. (2015). Toward the theory of the supply chain. *Journal of Supply Chain Management, 52*(2), 89–97.

Christopher, M., & Peck, H. (2004a). Building the resilient supply chain. *International Journal of Logistics Management, 15*(2), 1–14.

Christopher, M., & Peck, H. (2004b). The five principles of supply chain resilience. *Logistics Europe, 12*(1), 16–21.

Craighead, C. W., Blackhurst, J., Rungtusanatham, M. J., & Handfield, R. B. (2007). The severity of supply chain disruptions: Design characteristics and mitigation capabilities. *Decision Sciences, 38*(1), 131–156.

Durach, C. F., Wieland, A., & Machuca, J. A. D. (2015). Antecedents and dimensions of supply chain robustness: A systematic literature review. *International Journal of Physical Distribution & Logistics Management, 45*(1), 118–137.

Ellis, S., Henry, R., & Shockley, J. (2010). Buyer perceptions of supply disruption risk: A behavioral view and empirical assessment. *Journal of Operations Management, 28*(1), 34–46.

Hamel, G., & Välikangas, L. (2003). The quest for resilience. *Harvard Business Review, 81,* 52–63.

Handfield, R. B., & Bechtel, C. (2002). The role of trust and relationship structure in improving supply chain responsiveness. *Industrial Marketing Management, 31*(4), 367–382.

Hendricks, K. B., & Singhal, V. R. (2005). An empirical analysis of the effect of supply chain disruptions on long-run stock price performance and equity risk of the firm. *Production and Operations Management, 14*(1), 35–52.

Hohenstein, N.-O., Feisel, E., Hartmann, E., Giunipero, L. (2015). Research on the phenomenon of supply chain resilience: a systematic review and paths for further investigation. *International Journal of Physical Distribution & Logistics Management*, *45*(1), 90–117.

Jüttner, U., & Maklan, S. (2011). Supply chain resilience in the global financial crisis: An empirical study. *Supply Chain Management: An International Journal, 16*(4), 246–259.

Kamalahmadi, M., & Parast, M. M. (2016). A review of the literature on the principles of enterprise and supply chain resilience: Major findings and directions for future research. *International Journal of Production Economics, 171,* 116–133.

Knemeyer, M., Zinn, W., & Eroglu, C. (2009). Proactive planning for catastrophic events in supply chains. *Journal of Operations Management, 27*(2), 141–153.

Norrman, A., & Jansson, U. (2004). Ericsson's proactive supply chain risk management approach after a serious sub-supplier accident. *International Journal of Physical Distribution & Logistics Management, 34*(5), 434–456.

Pettit, T. J., Fiksel, J., & Croxton, K. L. (2010). Ensuring supply chain resilience: Development of conceptual framework. *Journal of Business Logistics, 31*(1), 1–21.

Ponomarov, S. Y., & Holcomb, M. C. (2009). Understanding the concept of supply chain resilience. *The International Journal of Logistics Management, 20*(1), 124–143.

Rice, J. B., & Caniato, F. (2003). Building a secure and resilient supply network. *Supply Chain Management Review, 7*(5), 22–30.

Sheffi, Y., & Rice, J. B. (2005). A supply chain view of the resilient enterprise. *MIT Sloan Management Review, 47*(1), 41–48.
Simchi-Levi, D. (2015). Find the weak link in your supply chain. *Harvard Business Review*.
Spekman, R. E. (1988). Strategic supplier selection: Understanding long-term buyer relationships. *Business Horizons, 31*(4), 75–81.
Tang, C. (2006). Perspectives in supply chain risk management. *International Journal of Production Economics, 103*(2), 451–488.
Tierney, K., & Bruneau, M. (2007). Conceptualizing and measuring resilience: A key to disaster loss reduction. *TR News*, 14–17.
Tukamuhabwa, B. R., Stevenson, M., Busby, J., & Zorzini, M. (2015). Supply chain resilience: Definition, review and theoretical foundations for further study. *International Journal of Production Research, 53*(18), 5592–5623.
Upton, D. M. (1997). Process range in manufacturing: An empirical study of flexibility. *Management Science, 43*(8), 1079–1092.
Wakolbinger, T., & Cruz, J. (2011). Supply chain disruption risk management through strategic information acquisition and sharing and risk-sharing contracts. *International Journal of Production Research, 49*(13), 4063–4084.
Wieland, A., & Wallenburg, C. M. (2013). The influence of relational competencies on supply chain resilience: A relational view. *International Journal of Physical Distribution & Logistics Management, 43*(4), 300–320.
Yao, Y., & Meurier, B. (2012). Understanding the supply chain resilience: A dynamic capabilities approach. In *9es Rencontres Internationales De La Recherche En Logistique* (pp. 1–17).

Part III
Incorporating Relational and Behavioral Perspectives

Chapter 11
Can Buyer Consortiums Improve Supplier Compliance?

Felipe Caro, Prashant Chintapalli, Kumar Rajaram and Christopher S. Tang

1 Introduction

Rising labor costs in the West have encouraged more firms to gradually source their products from other low-cost countries in the East. As more contract manufacturers compete for orders at lower prices in these countries, many factory owners cut corners to reduce their upfront investments and operating costs. In some cases, factory owners may even sacrifice product or process safety by not complying with product regulations or environmental and work safety codes. In terms of product safety violations, Tang and Babich (2014) report that some Chinese manufacturers committed product adulteration by using unsafe product materials. Examples include the use of melamine in milk and pet food products, ethanol in alcohol, lead-tainted paints in toys. In terms of environmental and work safety violations in China, the reader is referred to various reports developed by the Institute of Public and Environmental Affairs (IPE) for details (http://www.ipe.org.cn/en/about/report.aspx).

Bangladesh is an attractive country for Western companies (e.g., Walmart, H&M, Mango, and Adidas) to source apparel products due to its low labor cost (US $2 per day). However, without strong enforcement from the Bangladesh government and without strong commitment from buyers, many factory owners simply ignore health and safety issues at their factories. For example, due to the negligence of the factory owner, the collapse of Rana Plaza in Bangladesh killed over 1,000 apparel factory workers in 2013. While many international brands (Tommy Hilfiger, Gap, and several others) have contributed toward a fund for victims' relatives, the negative publicity caused major concerns for these companies that source from Bangladesh.

F. Caro (✉) · P. Chintapalli · K. Rajaram · C. S. Tang
UCLA Anderson School of Management, University of California,
Los Angeles, CA 90095, USA
e-mail: felipe.caro@anderson.ucla.edu

P. Chintapalli
Indian Institute of Management Bangalore, Bengaluru 560 076, India

G. A. Zsidisin and M. Henke (eds.), *Revisiting Supply Chain Risk*, Springer Series
in Supply Chain Management 7, https://doi.org/10.1007/978-3-030-03813-7_11

Donaldson (2014) commented that there is a perception that 20% of the factories in Bangladesh are unsafe in terms of building structure safety, fire safety, electrical safety, etc. Besides Bangladesh, many developing countries such as China, Cambodia, and Vietnam are facing similar challenges from non-compliant suppliers with unsafe factories. In 2013, a shoe factory collapsed killing three workers in Cambodia (Fuller and Bradsher 2013). Later, in 2014, a car parts factory explosion near Shanghai killed 68 workers (Demick 2013). In August 2015, a Tianjin warehouse overloaded with toxic chemicals such as sodium cyanide exploded killing over 114 people and injuring over 700 people (Wong and Fung 2015).

While international brands are not directly and legally responsible for their suppliers' workers' safety, there is a perceived collateral damage to their image. As articulated in Tang (2013), the brands listed earlier face a dilemma. If they stop sourcing from Bangladesh, millions of poor Bangladeshi workers will be out of work, especially because the garment industry accounts for 80% of the country's exports. On the other hand, if the brands continue to source from Bangladesh, there is a moral obligation to improve work safety at various factories. However, ensuring compliance is challenging as there are thousands of factories that are involved in different supply chain operations ranging from weaving, dyeing, and cutting to sewing. Recently, to address these challenges pertaining to compliance, many companies are forming specific units to ensure workplace safety at their suppliers' factories by conducting ***independent*** audits. For example, PVH Corp., the parent company of Calvin Klein, Tommy Hilfiger, and other such brands, increased their efforts in auditing supplier factories. Since 2012, PVH audits 84% of its tier-1 suppliers at least once per year and reports the non-compliant health and safety issues on its Web site (www.pvhcsr.com). While it is common for firms (or buyers) to conduct independent audits and penalize non-compliant suppliers, this mechanism has two drawbacks: (a) the audit process can be costly and time-consuming; and (b) the penalty imposed by an individual buyer may not be severe enough to entice suppliers to increase compliance especially when the supplier has many customers (i.e., buyers).

To overcome these two drawbacks and to show commitment for improving supplier compliance, firms are now considering forming consortiums and conducting ***joint*** audits so that they can share the audit cost and they can impose a collective penalty on non-compliant suppliers. One such example is the Accord on Fire and Building Safety in Bangladesh (http://www.bangladeshaccord.org). The Accord is a legally binding agreement signed in May 2013 by 166 apparel corporations from 20 countries in Europe, North America, Asia, and Australia, along with numerous Bangladeshi unions and NGOs (e.g., Workers Rights Consortium, International Labor Organization). The goal of the Accord is to improve workplace safety for over 2 million workers at 1,800 factories (Kapner and Banjo 2013).[1] Specifically, the Accord represents a consortium of companies and on their behalf selects impartial inspectors (with fire and building safety expertise), conducts thorough safety inspections of supplier factories, releases inspection reports to the public, imposes

[1]To reduce the exposure to broad legal liability, Walmart, Target, and other US retailers are developing a different accord for improving factory safety.

corrective actions to the non-compliant factories, and "jointly terminates" the business relationship when a non-compliant supplier is found committing serious safety violations, or when a non-compliant supplier fails to participate fully in the inspection and remediation (Caro and Tang 2014).

There are trade-offs between independent audits and joint audits. Independent audits enable each firm to fully control its own audit effort, but an individual firm can only impose a limited individual penalty on a non-compliant supplier, especially when the supplier conducts business with multiple firms. On the other hand, joint audits can enable a group of firms to impose a more severe collective penalty that can put a non-compliant supplier out of business. Moreover, due to the substitution effects between the audits of the two buyers, there is a possibility of free-riding between the buyers under independent audits, especially when the audit costs are high. On the other hand, joint audits can degrade channel profit when audit costs are high.

These trade-offs motivated us to examine the following questions when each buyer (firm) is concerned about its brand or collateral damage due to supplier's non-compliance:

1. Relative to individual audits, will joint audits result in a higher supplier compliance level? Will they result in lower buyer audit effort?
2. Which audit mechanism will generate higher payoffs for the firms, the supplier, and for the entire supply chain?

To study these questions, we develop a stylized model that involves three players (two buyers and one supplier) and captures the essence of both independent and joint audits. For each audit mechanism, we formulate a sequential-move game in which the two buyers will first select their audit levels simultaneously under the independent audits (and jointly under the joint audits). Upon observing (or anticipating) the buyer's audit level, the supplier selects its compliance level.

A sequential game better models those supply chains in which the buyers are substantially more powerful than the suppliers. In the examples that we cited to motivate our research, the international brands are substantially more powerful than the suppliers in developing countries from which the brands source their products. However, note that in our model we assume that buyers are similar and have equal market power so that the interactions between the buyers can be modeled through a simultaneous game. Thus, we adopt a mixture of a simultaneous-move game (between the buyers) and a sequential-move game (between the group of buyers and the supplier) to take our model as close to reality as possible. The analysis of a simultaneous-move game that is more applicable to a supply chain in which all the players (i.e., the buyers and the supplier) are equally powerful can be found in Caro et al. (2018). In this chapter, we restrict our attention to the sequential game.

Our analysis of the equilibrium outcomes reveals that relative to the independent audit mechanism, the joint audit mechanism can make the supplier increase its compliance level. Also, when the buyer's audit cost is below a certain threshold, we find that joint audit can increase the supply chain profit (i.e., the total profit of the buyers and supplier) so that one can devise a transfer payment system to ensure that joint auditing is Pareto-improving (i.e., all parties are better off under joint audit). Hence, our analysis reveals that joint audits can be Pareto-improving when the buyer's audit cost is low, but it is practical to adopt independent audits when the buyer's audit cost is high. This result appears to be counterintuitive because one would have expected that, by splitting the joint audit cost, the joint mechanism would dominate the independent mechanism in terms of supply chain profit. However, due to the strategic interaction among the buyers and the supplier, we find that this intuition turns out to be incorrect.

Our work falls within supply-chain risk management—a new research stream that has drawn significant interest among practitioners and researchers in recent years (Sodhi et al. 2012). The rising interest in supply-chain risk management is triggered by three types of supply chain disruptions. The first type is due to disruptions caused by natural disasters (Japan's Tōhoku earthquake and tsunami, Thailand's major flood, etc.) and man-made disasters such as the September 11 attacks. Chopra and Sodhi (2004) examine different mechanisms to mitigate various types of supply chain disruptions, Tomlin (2006) examines the implications of dual sourcing when one of the suppliers is unreliable, and Tang (2006) provides different strategies for mitigating supply chain risks. Hendricks and Singhal (2005) examine the impact of supply chain disruptions on a firm's stock returns. The reader is referred to a recent book by Sodhi and Tang (2012) for a comprehensive discussion on this kind of supply chain disruptions. The second type of disruptions is due to major financial crises (e.g., Asian currency devaluations in 1997, the sub-prime financial crisis in 2008) that can disrupt a supplier's operations. In the operations management (OM) literature, Babich et al. (2007) is one of the first to examine the issue of managing a portfolio of suppliers who face default risks.

Our work considers the third type of supply chain disruptions that are caused by a deliberate act committed by a supplier. Some recent research examines the issue of product adulteration that occurs when suppliers use unsafe materials to produce certain products that can cause physical harm to consumers. Well-publicized examples include Mattel's lead-tainted toys in 2007, melamine-tainted milk in 2008, and Baxter's adulterated Heperin in 2008. In the OM literature, Babich and Tang (2012) present a model to show that a firm can deter suppliers from committing product adulteration by deferring some of its payments so that the supplier can claim these payments only when no adulteration is found within a certain period of time. Rui and Lai (2015) find that the deferred payment strategy continues to be effective under more general conditions. More recently, after the IPE in Beijing exposed various factories dumping toxic waste in the water system in China and after the collapse of the Rana Plaza in 2013, the public expressed serious concern about suppliers' compliance with environmental and work safety regulations. This has put pressure on many Western firms to take action to improve supplier compliance. In this setting, Plambeck and Taylor (2015) use a game-theoretic model to explore the interactions between one buyer's audit level and one supplier's compliance and deception levels. By examining the equilibrium outcomes (supplier's compliance level, supplier's deception level, and buyer's audit level), they show that when a supplier deceives the auditors by hiding certain critical information, the buyer's actions (increasing audit level, paying a higher price, etc.) could motivate the supplier to cause more harm. In the context of environmental violations, Kim (2015) examines the interactions between the regulator's inspection policy and the firm's non-compliance disclosure timing decisions. By considering the case when environmental violations are stochastic, the author shows that there are conditions under which periodic inspection can be more effective than random inspection. Orsdemir et al. (2015) investigate how vertical integration can be used as a strategy to ensure compliance. They examine the scenario of two supply chains, one of which is vertically integrated, and highlight that the presence of a supply chain partnership plays a key role in determining supplier compliance. They argue that, in the absence of a partnership, overly tight violation scrutiny can backfire and degrade compliance when negative reporting externalities are high. In the presence of a supply chain partnership, the vertically integrated supply chain will cease to share responsibly sourced components with the non-integrated supply chain, despite the fact that the former benefits substantially from the exposure of the violations of the latter.

While our research also deals with the issue of supplier compliance, it is fundamentally different from those in the extant literature on supply-chain risk management in two ways. First, the above-listed papers primarily focus on the strategic interaction between one buyer and one supplier. Instead, we examine and compare independent and joint audit mechanisms by capturing the strategic interactions among two buyers and one potentially non-compliant supplier. Second, we recognize the issue of a non-compliant supplier and employ the notion of "collective penalty" imposed by both buyers when the non-compliant supplier fails the joint audits. Our contribution is to examine the implications of a collective penalty facilitated by the joint mechanisms.[2]

This chapter is organized as follows. In Sect. 2, we present our modeling framework and the resulting equilibrium outcomes associated with the independent and the joint audit mechanisms. In Sect. 3, we compare the equilibrium outcomes associated with these audit mechanisms. We present our conclusions in Sect. 4. All proofs are provided in the Appendix.

2 The Model

Consider a supply chain comprising of two buyers ($i = 1, 2$) and one supplier s. For ease of exposition, we consider the case when buyer i sells one unit of its product at price p_i and pays the supplier a wholesale price w_i. We denote the supplier's unit cost by c_i. Since our focus is on the audit mechanism, we consider p_i, w_i, and c_i to be exogenous so that the values of these parameters do not depend on the audit

[2] An alternative audit mechanism is the ***shared*** audit mechanism in which the buyers conduct their audits independently, but share their audit reports eventually. We omit the discussion of the shared audit mechanism in this chapter due to space considerations. We refer the reader to (Caro et al. 2015) for the analysis of shared audits.

mechanism adopted by the buyers. In other words, the strategic intent of different audit mechanisms is to encourage the supplier to improve its compliance level, but not to increase selling prices or reduce wholesale prices (e.g., Van Mieghem 1999) or both. This seems reasonable in the context of outsourcing agreements between Western firms and suppliers located in developing countries because reducing the wholesale price would create public concerns about the firm's moral and ethical standards. Also, for the reason of tractability and given that the focus of our research is to examine and compare the performance of different audit mechanisms, we shall defer the case of endogenous wholesale price w_i to future research.

We use a sequential-move game to model the dynamics between the buyers and the supplier: The buyers (e.g., international brands) are the leaders and the supplier is the follower that decides whether to comply or not. This sequence of events is representative of many global supply chains in which the buyers have a stronger position to set the sourcing terms. First, under independent audits, each buyer i selects its audit level z_i, $i = 1, 2$ simultaneously and incurs an audit cost of αz_i^2, where $\alpha > 0$ and $z_i \in [0, 1]$. Here, z_i represents the probability that buyer i will conduct the audit. This notion of audit probability is commonly used in the literature (e.g., Babich and Tang 2012; Plambeck and Taylor 2015). Under joint audits, both buyers exert the joint audit level $z \in [0, 1]$ and split the audit cost αz^2 between them. Upon observing the buyers' audit levels, the supplier selects its compliance level x and incurs a compliance cost γx^2, where $\gamma > 0$ and $x \in [0, 1]$. Here, x represents the probability that the supplier complies with the (environmental, workplace, and product safety) regulations. To facilitate the comparison of the supplier's compliance level and the supply chain profit across the two audit mechanisms, we shall assume that the audit cost α remains the same across both the mechanisms (even though the same approach can be applied to examine the case when the audit cost depends on the underlying audit mechanism). Also, for tractability, we do not consider the issue of supplier deception, i.e., the supplier choosing the effort level to deceive the buyers, the phenomenon that was introduced by Plambeck and Taylor (2015).

Regardless of the audit mechanism adopted by the buyers, all parties face the following risks (see Fig. 1). First, if a non-compliant supplier is identified by buyer i, buyer i will reject the unit without paying, and the supplier will incur a goodwill cost g_i associated with contract termination imposed by buyer i. Second, if a non-compliant supplier is not identified by buyer i, buyer i will accept the unit and pays the supplier w_i. However, there is a chance that this non-compliance will be exposed to the public. In that case, buyer i will incur an expected "collateral damage" d_i due to the spillover effect of the non-compliant supplier. Throughout this chapter, we shall assume that the collateral damage d_i is severe enough so that there is an incentive for a buyer to audit its supplier. For this reason, we make the following two assumptions that provide motivation for the supplier to care about compliance and for the buyer to care about auditing:

Assumption 1 The supplier's goodwill cost g_i associated with contract termination imposed by buyer i is higher than the supplier's corresponding profit margin so that $g_i > (w_i - c_i)$ for $i = 1, 2$.

Assumption 2 Buyer i's damage cost d_i associated with a non-compliant supplier is higher than the buyer's profit margin so that $d_i > (p_i - w_i) \equiv m_i$ for $i = 1, 2$.

2.1 Independent Audits (I)

We now analyze the sequential-move game under the independent audits by using backward induction. Specifically, we first analyze the supplier's best response compliance level $x^*(z_1, z_2)$ for any given audit levels (z_1, z_2) selected by the buyers. Anticipating the supplier's best response, we analyze a noncooperative game in which both buyers select their own audit levels (z_1, z_2) simultaneously. We can then obtain the equilibrium outcomes via substitutions.

From Fig. 1, we observe that the supplier will fail buyer i's audit with probability $z_i(1 - x)$ under independent audits. By considering the wholesale price w_i, the goodwill cost g_i, and the compliance cost γx^2, the supplier's problem for any given audit level (z_1, z_2) is:

$$\begin{aligned}\pi_s(z_1, z_2) &= \max_{x\in[0,1]} \sum_{i=1}^{2} [w_i(1 - z_i(1 - x)) - g_i z_i(1 - x) - c_i] - \gamma x^2 \\ &= \max_{x\in[0,1]} \sum_{i=1}^{2}(w_i - c_i) - \sum_{i=1}^{2}(w_i + g_i) z_i(1 - x) - \gamma x^2. \end{aligned} \tag{1}$$

To ensure that the supplier has incentive to fully comply and that the compliance level captures the entire range from 0 to 1, we assume that the supplier's profit margin is high enough so that the supplier's expected profit is nonnegative under full compliance (i.e., when $x = 1$). By considering the objective function given in (1), this assumption can be stated as:

Assumption 3 The supplier's total profit margin is higher than his full compliance cost so that $\sum_{i=1}^{2}(w_i - c_i) \geq \gamma$.

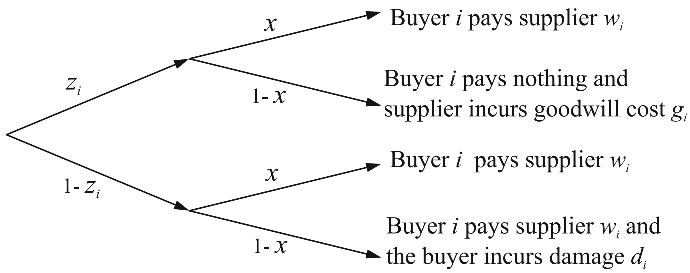


Fig. 1 Independent audit: buyer i's audit level z_i and supplier's compliance level x

Before determining the supplier's best response, we first consider the case when the buyers conduct full audit so that $(z_1, z_2) = (1, 1)$. In this case, the derivative of the supplier's profit given in (1) with respect to its compliance level x is equal to $\sum_{i=1}^{2}(w_i + g_i) - 2\gamma x$. Hence, if we consider $(w_i + g_i)$ as the supplier's gain for increasing its compliance level by investing 2γ per unit of compliance, then we can interpret the term $r_i \equiv \frac{w_i+g_i}{2\gamma}$ as the supplier's "rate of return on compliance from buyer i." Also, by applying Assumptions 1 and 3, it is easy to check that $\sum_{i=1}^{2} g_i \geq \sum_{i=1}^{2}(w_i - c_i) \geq \gamma$ and that $\sum_{i=1}^{2} w_i \geq \gamma$. Hence, we can conclude that: $\sum_{i=1}^{2} \frac{w_i+g_i}{2\gamma} = r_1 + r_2 \geq 1$. As we shall see, r_i will be useful in interpreting our results later and the condition $r_1 + r_2 \geq 1$ will be employed in some of the proofs.

By using the first-order condition associated with (1), the supplier's best response compliance level $x^*(z_1, z_2)$ and the corresponding payoff $\pi_s(z_1, z_2)$ are given by:

$$x^*(z_1, z_2) = \min\left\{\frac{\sum_{i=1}^{2}(w_i + g_i)z_i}{2\gamma}, 1\right\} = \min\left\{\sum_{i=1}^{2} r_i z_i, 1\right\}, \text{ and} \tag{2}$$

$$\pi_s(z_1, z_2) = \sum_{i=1}^{2}(w_i - c_i) - \gamma + \gamma(1 - x^*)^2 \geq 0, \tag{3}$$

where the last inequality is due to Assumption 3. Observe from (2) that, for any given audit levels (z_1, z_2), the supplier's compliance level $x^*(z_1, z_2)$ is based only on the rate of returns on compliance r_i and the buyer's audit level z_i. Hence, the higher the audit level z_i each buyer is willing to employ, the higher is the supplier's compliance level x. Thus, it follows from Assumption 3 and (3) that the supplier's participation constraint $\pi_s(z_1, z_2) \geq 0$ is always satisfied. This result is due to the fact that the supplier can always select its compliance level x to ensure that its profit is nonnegative.

Given the supplier's best response, we now analyze the buyer's problem in which both buyers select their audit levels (z_1, z_2) simultaneously in a noncooperative manner. Buyer i maximizes its expected profit and selects its audit level z_i for a given audit level z_j of buyer j. Upon investing αz_i^2, buyer i earns m_i (i.e., the profit margin $m_i \equiv (p_i - w_i)$) if the supplier passes the audit with probability $(1 - z_i(1 - x^*))$. At the same time, buyer i is exposed to the collateral damage d_i if the non-compliant supplier passes the audit with probability $(1 - z_i)(1 - x^*)$. For any given audit level z_j of buyer j, buyer i's problem can be formulated as follows:

$$\Pi_i(z_j) = \max_{z_i \in [0,1]} \{m_i(1 - z_i(1 - x^*)) - \alpha z_i^2 - d_i(1 - z_i)(1 - x^*)\} \tag{4}$$
$$\text{s.t. } (2).$$

Since $\alpha > 0$, the objective function is concave in z_i. By examining the first-order condition, Eq. (2), and the upper bound on z_i, the buyer i's best response audit level $z_i^*(z_j)$ is given by:

$$z_i^*(z_j) = \min\left\{\frac{d_i r_i + (d_i - m_i)(1 - r_j z_j)}{2(\alpha + (d_i - m_i) r_i)}, \frac{1 - r_j z_j}{r_i}, 1\right\}.$$

Observe that the audit efforts are substitutes: buyer i's audit level $z_i^*(z_j)$ decreases when buyer j's audit level z_j increases. In addition, it is easy to check that, when α is high enough, buyer i's audit level is an interior solution so that:

$$z_i^* = \frac{2(d_i r_i + (d_i - m_i))(\alpha + (d_j - m_j) r_j) - (d_i - m_i) r_j \cdot (d_j r_j + (d_j - m_j))}{4(\alpha + (d_i - m_i) r_i)(\alpha + (d_j - m_j) r_j) - (d_i - m_i) r_i \cdot (d_j - m_j) r_j},$$
$$\text{for } i = 1, 2. \tag{5}$$

The complex expression (5) is not amenable to closed-form analysis. For this reason, we consider the case of symmetric buyers so that $p_i = p_j = p$, $d_i = d_j = d$, $w_i = w_j = w$, $c_i = c_j = c$, $m_i = m_j = m$, and $r_i = r_j = r$. Thus, $r_1 + r_2 \geq 1$ is now simplified to $2r \geq 1$. In this case, Eqs. (2) and (5) imply that, in equilibrium, the buyer's audit level z^I and the supplier's compliance level x^I under the independent audit mechanism can be expressed as[3]:

$$z^I = \begin{cases} \frac{dr + (d-m)}{2\alpha + 3r(d-m)} & \text{if } \alpha \geq \beta \\ \frac{1}{2r} & \text{if } \alpha < \beta \end{cases} \quad \text{and} \quad x^I = \begin{cases} 2r\frac{dr + (d-m)}{2\alpha + 3r(d-m)} & \text{if } \alpha \geq \beta \\ 1 & \text{if } \alpha < \beta, \end{cases} \tag{6}$$

where

$$\beta \equiv \frac{2dr^2 - r(d-m)}{2}. \tag{7}$$

Using Assumptions 1–3 to examine the buyer's equilibrium audit level z^I and the supplier's equilibrium compliance level x^I given in (6), and using the fact that $2r \geq 1$ when both buyers are identical, we obtain the following results:

Lemma 1 *Under the independent audit mechanism I, the buyer's audit level z^I and the supplier's compliance level x^I given in* (6) *possess the following properties:*

1. *The supplier's compliance level is higher than the buyer's audit level: $x^I = 2rz^I \geq z^I$.*
2. *Both z^I and x^I are increasing in the buyer's damage cost d.*
3. *Both z^I and x^I are decreasing in the buyer's audit cost α.*
4. *The supplier's compliance level x^I is decreasing in the supplier's compliance cost γ.*
5. *When the buyer's audit cost α is low (high), the buyer's audit level z^I increases (decreases) as the supplier's compliance cost γ increases.*

Lemma 1 has the following implications. Because the supplier's compliance level $x^I = 2r \cdot z^I$, it suffices to focus on the buyer's audit level z^I given in (6). The first

[3]Throughout this chapter, we shall use the superscripts I and J to denote the equilibrium outcomes under independent and joint audits, respectively.

statement reveals that, under the independent audit mechanism, the buyer's audit has an amplifying effect: It can trigger the supplier to increase its compliance level by the factor of $2r(\geq 1)$ (i.e., twice the rate of return on compliance). Consequently, the first statement implies that the buyer can encourage the supplier to comply fully without conducting full audits (i.e., $z_i < 1$). The second statement is intuitive. Due to concerns over the damage cost d, the buyers will increase their audit levels as d increases, which will in turn forces the supplier to increase its compliance level. In the same vein, the audit cost has a dampening effect: Higher audit cost will force the buyers to reduce their audit levels, which leads to the supplier reducing its compliance level. The fourth statement can be interpreted in the same way.

The fifth statement requires some discussion. First, when the audit cost is low, the buyer can afford to increase its audit level to ensure that the supplier will sustain its (full) compliance level as γ increases. However, when α is high, the buyer is concerned about the rising audit cost. Under independent audits, each buyer has incentive to "free ride" on the other buyer's audit level due to the underlying substitution effect as observed in the best response function $z_i^*(z_j)$. This effect leads each buyer to shirk and reduce its audit level as gamma increases in order to compensate for the higher expected collateral damage due to the supplier's lower compliance level.

By substituting z^I given in (6) into (4) and (3), we obtain the buyer's profit $\Pi^I(z^I)$ and the supplier's profit $\pi_s^I(z^I)$ under the independent audit mechanism, as follows:

$$\Pi^I(z^I) = m(1 - z^I(1 - 2r \cdot z^I)) - \alpha(z^I)^2 - d(1 - z^I)(1 - 2r \cdot z^I), \text{ and} \quad (8)$$

$$\pi_s^I(z^I) = 2(w - c) - \gamma + \gamma(1 - 2r \cdot z^I)^2. \quad (9)$$

By using $x^I, z^I, \Pi^I(z^I)$, and $\pi_s^I(z^I)$ that are associated with the independent mechanism as benchmarks, we next examine the joint audit mechanism.

2.2 Joint Audits (J)

We now analyze the sequential-move game associated with joint audits using backward induction. Consider the supplier's problem for any given joint audit level z that is simultaneously selected by both buyers. In this case, the supplier will fail the joint audit with probability $z(1 - x)$. Upon failing the joint audit, the supplier receives no payment and will be subject to a collective penalty of $(g_1 + g_2)$ that is imposed by both the buyers together. Hence, the supplier solves:

$$\pi_s(z) = \max_{x \in [0,1]} \{[(w_1 + w_2)(1 - z(1 - x)) - (g_1 + g_2)z(1 - x) - (c_1 + c_2)] - \gamma x^2\}.$$

From the first-order condition, the supplier's best response $x(z)$ and its corresponding payoff $\pi_s(z)$ can be expressed as:

$$x^*(z) = \min\{(r_1 + r_2)z, 1\} \text{ and} \tag{10}$$

$$\pi_s(z) = \sum_{i=1}^{2}(w_i - c_i) - \gamma + \gamma(1 - x^*)^2 \geq 0, \tag{11}$$

where $r_i \equiv \frac{(w_i+g_i)}{2\gamma}$ for $i = 1, 2$.

Analogous to the independent audit case, (10) reveals that the supplier's best response $x^*(z)$ is equal to the rate of return on compliance times the joint audit level. Also, as in the independent case, Eq. (11) shows that the supplier's participation constraint $\pi_s(z) \geq 0$ is always satisfied due to Assumption 3. Comparing Eqs. (2) and (10), we notice that the supplier's compliance level will be the same under both independent and joint audit mechanisms if $z = z_1 = z_2$.

Now, we examine the buyers' problem under joint audits. Due to the complexity of the buyers' problem, we shall focus on the case of symmetric buyers. In this case, it is easy to check from (10) that $x^* = 2rz$ because there is no incentive for the buyer to set the audit level $z > \frac{1}{2r}$.

Akin to the independent audit mechanism, the buyers join a consortium to maximize their individual payoffs and independently decide on the joint audit level z and the apportionment of the audit cost αz^2 between themselves. Following Harsanyi (1982b), we shall model the audit level decision and the audit cost allocation as a simultaneous-move noncooperative unanimity game in which each buyer i proposes an audit level and a split of the audit cost. If the buyers' proposed audit levels are identical, and the sum of the buyers' shares of the audit cost equals 1, the joint audit mechanism will be implemented; otherwise, the negotiations break down and buyers will resort to independent audits and earn Π^I given in (8). More formally, let z_i and θ_i represent the audit level and the share of audit cost proposed by buyer i. By considering each buyer's payoff using (4) and the fact that $x^* = 2rz$, we can check that the equilibrium $(\tilde{z}_i, \tilde{\theta}_i)$ in the simultaneous-move noncooperative unanimity game is given by:

$$(\tilde{z}_i, \tilde{\theta}_i) = \arg\max \left\{U(z_i, \theta_i; z_j, \theta_j) : \ z_i, \theta_i \in [0, 1]\right\}, \text{ where}$$

$$U(z_i, \theta_i; z_j, \theta_j) = \begin{cases} m(1 - z_i(1 - 2rz_i)) - d(1 - z_i)(1 - 2rz_i) - \theta_i \alpha z_i^2 & \text{if } z_i = z_j, \theta_i + \theta_j = 1; \\ \Pi^I & \text{otherwise,} \end{cases}$$

for $i = 1, 2$ and $i \neq j$. Due to the condition $z_1 = z_2$ and $\theta_1 + \theta_2 = 1$, we know that there exists an infinite number of equilibrium points to the above unanimity game. To select choose one equilibrium point, we adopt the payoff-dominance selection rule proposed by Harsanyi and Selten (Harsanyi 1982a).[4] Specifically, Harsanyi (1982b)

[4]As defined by Harsanyi (1982b), a "payoff-dominant" equilibrium is Pareto superior to all other equilibria. Therefore, when faced with a choice among equilibria, the payoff-dominance selection rule assumes that all players would agree on the payoff-dominant equilibrium since it offers to each player at least as much payoff as the other equilibria. The rule is also shown to be risk dominant.

shows that the payoff-dominant solution to this noncooperative game solves the following optimization problem:

$$\max_{z,\theta_1\in[0,1]} [m(1-z(1-2rz)) - d(1-z)(1-2rz) - \theta_1\alpha z^2 - \Pi^I]\cdot \\ [m(1-z(1-2rz)) - d(1-z)(1-2rz) - (1-\theta_1)\alpha z^2 - \Pi^I], \qquad (12)$$

where θ_1 is the share of the joint audit cost to be borne by buyer 1.[5] In this case, it is easy to check that the optimal share is $\theta_1^* = 0.5$ and the equilibrium audit level z^J and the corresponding compliance level x^J satisfy:

$$z^J = \begin{cases} \frac{2dr+(d-m)}{\alpha+4r(d-m)} & \text{if } \alpha \geq 4\beta \\ \frac{1}{2r} & \text{if } \alpha < 4\beta \end{cases} \quad \text{and} \quad x^J = \begin{cases} 2r\frac{2dr+(d-m)}{\alpha+4r(d-m)} & \text{if } \alpha \geqslant 4\beta \\ 1 & \text{if } \alpha < 4\beta, \end{cases} \qquad (13)$$

where β is given in (7).

Using Assumptions 1–3 to examine the buyer's joint audit level z^J and the supplier's compliance level x^J given in (13), we obtain the following results:

Lemma 2 *Under the joint audit mechanism J, the buyer's joint audit level z^J and the supplier's compliance level x^J given in* (13) *possess the following properties:*

1. *The supplier's compliance level is higher than the buyer's audit level: $x^J = 2rz^J \geq z^J$.*
2. *Both z^J and x^J are increasing in the buyer's damage cost d.*
3. *Both z^J and x^J are decreasing in the buyer's audit cost α.*
4. *The supplier's compliance level x^J is decreasing in the supplier's compliance cost γ.*
5. *When the buyer's audit cost α is low (high), the buyer's audit level z^J increases (decreases) as the supplier's compliance cost γ increases.*

Because Lemma 2 is analogous to Lemma 1, we can interpret the results the same way as before. Also, because the supplier's compliance level $x^J = 2r \cdot z^J$, it suffices to focus on buyer's joint audit level z^J given in (13). Using Eqs. (11) and (13) , we obtain each buyer's profit $\Pi^J(z^J)$ and the supplier's profit $\pi_s^J(z^J)$ under the joint audit mechanism as:

$$\Pi^J(z^J) = m(1-z^J(1-2rz^J)) - d(1-z^J)(1-2rz^J) - \frac{\alpha}{2}(z^J)^2, \text{ and} \qquad (14)$$

$$\pi_s^J(z^J) = 2(w-c) - \gamma + \gamma(1-2r\cdot z^J)^2. \qquad (15)$$

[5] To maintain the consistency of each buyer's self-interest, our noncooperative unanimity game enables us to preserve the noncooperative framework throughout this chapter. If we were to adopt the nash bargaining (NB) solution concept in a cooperative framework, then it is easy to observe that this optimization problem will yield the same nash bargaining solution; see Harsanyi (1982b).

After establishing the expressions for x^J, z^J, $\Pi^I(z^J)$, and $\pi_s^I(z^J)$, we can now compare the equilibrium outcomes between the joint and the independent audit mechanisms.

3 Independent Versus Joint Audits Equilibrium Comparison

First, we use Assumptions 1–3 and the outcomes presented in (6) and (13) to compare the buyer's audit level and the supplier's compliance level under both mechanisms. We obtain the following result:

Proposition 3 *Relative to the independent audit mechanism, the buyer's audit level and the supplier's compliance level are higher under the joint audit mechanism:* $z^J \geq z^I$ *and* $x^J \geq x^I$.

Proposition 3 is intuitive. Under the joint mechanism, the buyers can afford to exert a higher joint audit level because the audit cost is shared. On the other hand, the supplier must commit to a higher compliance level under joint audits in response to an increased audit level and the higher (collective) penalty of non-compliance.

Second, we compare the supplier's profits as given in (9) and (15) to obtain the following result:

Proposition 4 *Relative to the independent audit mechanism, the supplier obtains a lower profit under the joint audit mechanism:* $\pi_s^J(z^J) \leq \pi_s^I(z^I)$.

Proposition 4 has the following implications. The supplier is worse off when the buyers exert a higher audit level and impose the collective penalty under the joint audit mechanism. We next examine the buyer's profit under joint audits. By direct comparison of each buyer's profit Π^J given in (14) and Π^I given in (8), we get:

Proposition 5 *Relative to the independent audit mechanism, the buyer obtains a higher profit under the joint mechanism:* $\Pi^J(z^J) \geq \Pi^I(z^I)$.

Proposition 5 shows that each buyer obtains a higher profit under the joint audit mechanism by sharing the audit cost and by imposing the collective penalty on the non-compliant supplier.

The contrasting results as stated in Propositions 4 and 5 create a challenge for the buyers to adopt joint audits. Even if the supplier is forced to participate in the joint audit mechanism, one would question the buyer's moral standard and the public may pressurize the buyers to treat the supplier fairly to ensure that the supplier is not worse off. Hence, the joint audit mechanism is viable only when it can be Pareto-improving so that the buyers and the supplier will not be worse off under joint audits.

The joint audit mechanism is Pareto-improving when the supply chain profit (i.e., the total profit of both buyers and the supplier) under joint audit is higher than the profit under independent audits so that there exists a payment transfer scheme from the buyers to the supplier to ensure that the supplier will not be worse off. Thus, we need to examine whether the supply chain profit will be higher under the joint audit mechanism. When $\alpha \leq \beta$, we know from Eqs. (6) and (13) that $z^I = z^J = \frac{1}{2r}$ and it can be shown that there is a gain of $\frac{\alpha}{4r^2}$ in the supply chain profit under the joint audit mechanism compared to the profit with independent audits. Hence, when the auditing cost α is sufficiently low, the supply chain profit will be higher in the joint audit regime. However, the comparison between the supply chain profits under the joint and independent audits when α is high is given in Proposition 6. Note that the supply chain profit under the joint mechanism is equal to $2 \cdot \Pi^J(z^J) + \pi_s^J(z^J)$, where $\Pi^J(z^J)$ and $\pi_s^J(z^J)$ are given in (14) and (15), and the profit under the independent audit mechanism is equal to $2 \cdot \Pi^I(z^I) + \pi_s^I(z^I)$, where $\Pi^I(z^I)$ and $\pi_s^I(z^I)$ are given in (8) and (9). Through direct comparison, we obtain the following result:

Proposition 6 *When the buyer's audit cost* α *is sufficiently high and the damage cost* d *and margin* m *are sufficiently small, the supply chain profit under the joint audit mechanism is lower than that under independent audits, i.e.,* $2 \cdot \Pi^J(z^J) + \pi_s^J(z^J) < 2 \cdot \Pi^I(z^I) + \pi_s^I(z^I)$.

We already argued that when the buyer's audit cost α is sufficiently low, the joint audit mechanism will increase the supply chain profit. With a higher supply chain profit, it is always possible for the buyers to work with the supplier to come up with a transfer payment scheme to ensure everyone is better off. Combining this observation along with Proposition 5, we can conclude that the joint audit mechanism can entice the supplier to increase its compliance level and it can be Pareto-improving as long as the buyer's audit cost α is below a certain threshold. When the buyer's audit cost α is high, Proposition 6 reveals that joint audits will yield a lower supply chain profit when the buyers' margins and damage costs are small. With a lower supply chain profit, the joint audit mechanism cannot be Pareto-improving and its implementation can be problematic. Therefore, despite the fact that the buyers split the audit cost, the joint audit mechanism is not always beneficial for the entire supply chain. Fortunately, for a wide range of parameter values the joint mechanism does improve the supply chain profit, as we show next.

We now illustrate our result numerically. Throughout the chapter, we set $w = 1100$, $g = 1110$, $c = 0$, $d = 1000$, $m = 800$, and we only vary the auditing cost α and the cost of compliance γ, which are the key parameters in the model. For $\gamma = 1700$, Figs. 2, 3, and 4 illustrate the results stated in Propositions 4, 5, and 6, respectively. To interpret Figs. 2, 3, and 4, first consider the case when the buyer's audit cost α is low. Specifically, when $\alpha < \beta$, (6) and (13) reveal that the supplier will fully comply so that $x^I = x^J = 1$ and each buyer will use the same audit level $z^I = z^J = \frac{1}{2r}$ under both audit mechanisms. With the same audit level under both audit mechanisms, Fig. 2 confirms that the supplier's profits are the same under both mechanisms. However, Fig. 3 shows that each buyer's profit is higher under the joint audit mechanism. This is because both buyers split the joint audit cost under joint audits instead of each buyer paying for its own audit cost under the independent audits.

Fig. 2 Supplier's profits under I and J ($\gamma = 1700$)

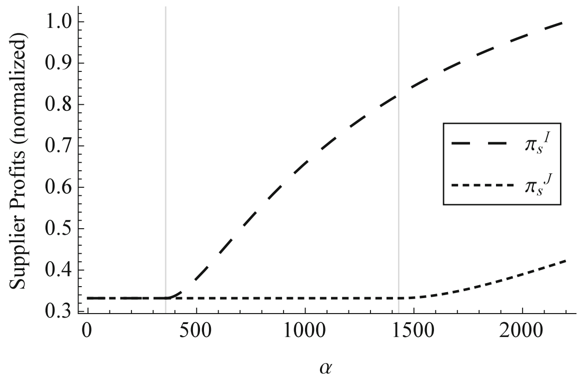


Fig. 3 Buyers' profits under I and J ($\gamma = 1700$)

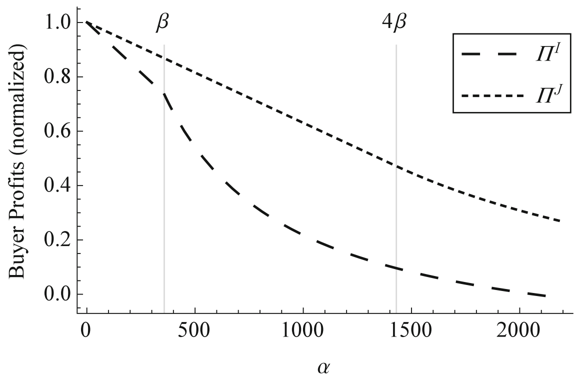
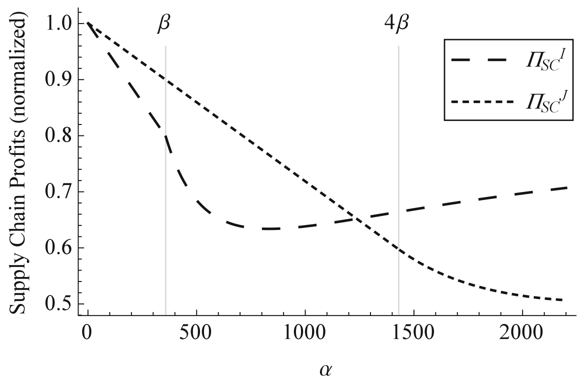


Fig. 4 Supply chain profits under I and J ($\gamma = 1700$)



Next, we consider the case when the buyer's audit cost α is high; for instance, when $\alpha > 4\beta$. In this case, Lemmas 1 and 2 imply that, when the buyer's audit cost α is high, the buyer will audit less and so the supplier will comply less. In particular, (6) and (13) reveal that the supplier will reduce its compliance level so that $x^I < x^J < 1$. At the same time, the buyer will reduce its audit level so that $0 < z^I < z^J < \frac{1}{2r}$. From the supplier's perspective, the supplier will earn a much higher profit under the independent audit because the probability that the supplier will fail the audit under an independent audit is lower than that under a joint audit when the buyer's audit cost becomes higher. Specifically, when $0 < z^I < z^J < \frac{1}{2r}$, the probability that the supplier will fail the audit is lower under the independent audit because $z^I(1 - x^I) = z^I(1 - 2rz^I) < z^J(1 - 2rz^J) = z^J(1 - x^J)$. This observation is reflected in Fig. 2, which illustrates that the supplier will earn a higher profit under the independent audit when the buyer's audit cost α is high.

From the buyer's perspective, the benefit of the joint audit mechanism over the independent audit becomes less significant at high values of α for two reasons: (a) The benefit of sharing the audit cost under the joint audit mechanism becomes less significant when the buyer audits less (because α is high); and (b) the benefit of the collective penalty under the joint audit mechanism becomes less significant when the buyer audit less (because α is high). Figure 3 shows that the buyer will experience an increased profit under a joint audit, but this increase in profit becomes smaller when α is high.

When α is high, the decrease in the supplier's profit (due to joint audits) appears to dominate the total increase in the buyers' profits (due to joint audits). Figure 4 confirms the statement of Proposition 6. The supply chain profit is lower under the joint audit mechanism when the buyer's audit cost α is sufficiently high. Hence, the joint audit mechanism cannot be Pareto-improving when auditing is too costly. However, when α is below a certain threshold, Fig. 4 shows that the joint audit mechanism can be Pareto-improving.

4 Conclusions

In this chapter, we investigate the impact of the independent and the joint audit mechanisms on supplier's compliance level by considering a stylized model that involves two buyers and one supplier. We employ a sequential game which better abstracts the strategic interactions in supply chains in which the buyers are substantially more powerful than the suppliers. The buyers move first through conducting audits and the suppliers move next by complying with the audits held. (We shall refer the reader to Caro et al. (2018) for the details about a simultaneous-move game model that is more applicable when both the buyers and the supplier are almost equally powerful.) Based on our examination of the equilibrium outcomes of the sequential game, we obtain the following results:

- Relative to the independent audit mechanism, the supplier will increase its compliance level under the joint mechanism, and the supplier will obtain a lower profit under the joint mechanism.
- Relative to the independent audit mechanism, the audit level is higher under the joint mechanism, and each buyer will obtain a higher profit under the joint mechanism.
- While the joint audit mechanism appears to be appealing, we find that joint audits can cause harm to the supply chain payoff (i.e., channel profit) especially when the buyers' audit costs are high.

In addition to gaining a better understanding of the impact of different audit mechanisms on the buyer's audit level and the supplier's compliance level, the above results have the following two practical implications:

1. When the audit cost is low, the joint mechanism can entice the supplier to increase its compliance level and this can be Pareto-improving (i.e., there exists a transfer payment scheme so that all parties will not be worse off.).
2. When the audit cost is high, the independent mechanism is the more practical option because the joint mechanism cannot be Pareto-improving.

Future research could consider alternate audit mechanisms and settings where our modeling assumptions do not apply. These include settings where the buyers are nonidentical (different price/cost structure, different bargaining power, etc.), or settings where information about price and cost structure is not perfectly known to all parties. Given the current concerns over supplier compliance, addressing those questions could be worthwhile avenues for future research.

Acknowledgements The authors would like to thank Professors Gregory Leblanc and Terry Taylor of University of California, Berkeley, for discussing the joint audit mechanism and the notion of collective penalty with one of the authors.

5 Appendix—Proofs

Proof of Lemma 1. The first statement follows from the fact that $2r \geq 1$ and (6). To prove the second statement, first observe that $z^I = \frac{x^I}{2r}$. Hence, it suffices to show the result for z^I and when $\alpha \geq \beta$ (otherwise, z^I is constant). In preparation, we claim that $\beta \geq \dfrac{3mr^2}{2(1+r)}$. To prove this claim, we apply (7) to show this equality holds if and only if $d(2r^2 + r - 1) + m(1 - 2r) \geq 0$. By using the fact that $2r \geq 1$ and by applying Assumption 2, we prove the claim by showing that $d(2r^2 + r - 1) + m(1 - 2r) \geq (d - m)(2r - 1) \geq 0$. Now we prove z^I is increasing in d for any $\alpha \geq \beta \geq \frac{3mr^2}{2(1+r)}$. By differentiating z^I with respect to d, z^I is indeed increasing in d because $\alpha \geq \frac{3mr^2}{2(1+r)}$. This proves the second statement. The third, fourth, and the fifth statements can be proven by direct differentiation with respect to α and γ, respectively. We omit the details. ■

Proof of Lemma 2. The proof follows the same approach as the proof for Lemma 1. We omit the details. ■

Proof of Proposition 3. Because $x^I = 2rz^I$ and $x^J = 2rz^J$, it suffices to show that $z^J \geq z^I$. From (6) and (13), $z^J \geq z^I$ if and only if $\frac{2dr+(d-m)}{\alpha+4r(d-m)} \geq \frac{dr+(d-m)}{2\alpha+3r(d-m)}$. This inequality holds when $3dr\alpha + \alpha(d-m) + r(d-m)\big(m + d(2r-1)\big) \geq 0$. This last inequality holds because $r \geq 1/2$ due to Assumptions 1–3. ■

Proof of Proposition 4. Observe from (9) and (15) that, after some algebra,

$$\begin{aligned}\pi_s^J(z^J) - \pi_s^I(z^I) &= 2(g+w)z^I - 4r(g+w){z^I}^2 - 2(g+w)z^J \\ &\quad + 4r(g+w){z^J}^2 + 4r^2({z^I}^2 - {z^J}^2)\gamma, \\ &= 2(g+w)\left[z^I(1-rz^I) - z^J(1-rz^J)\right] \leq 0. \qquad (16)\end{aligned}$$

The last inequality follows immediately by using three facts: (a) the parabola $y(1-ry)$ attains its maximum when $y = \frac{1}{2r}$; (b) $z^I \leq z^J$ (Proposition 3); and (c) both z^I and z^J are less than $\frac{1}{2r}$ (c.f. Eqs. (6) and (13)). ■

Proof of Proposition 5. By the assumption of individual rationality, the buyers operate under the joint audit mechanism only if $\Pi^J(z^J) \geq 0$.

Now, suppose that $0 \leq \Pi^J(z^J) < \Pi^J(z^I)$. Then $\big(\Pi^J(z^J) - \Pi^I\big)^2 < \big(\Pi^J(z^I) - \Pi^I\big)^2$, where Π^I are the profits if negotiations fail. But this would be a contradiction because z^J is the optimal solution to (12). Hence, $\Pi^J(z^J) \geq \Pi^J(z^I) = \Pi^I(z^I) + \frac{\alpha}{2}(z^I)^2 \geq \Pi^I(z^I)$ and the proof is complete. ■

Proof of Proposition 6. To compare the supply chain profit under both mechanisms, it suffices to examine the supply chain profit gap Δ_{SC}, where $\Delta_{SC} \equiv [2\Pi^J(z^J) + \pi_s^J(z^J)] - [2\Pi^I(z^I) + \pi_s^I(z^I)]$. After some algebra, we have that:

$$\begin{aligned}\Delta_{SC} &= \alpha(z^I)^2 + (z^J - z^I)\{2(d-m+2dr-2r\gamma) \\ &\quad - (z^J + z^I)(\alpha + 4r(d-m-r\gamma))\} \\ &= \alpha[\sqrt{2}\cdot z^I - z^J][\sqrt{2}\cdot z^I + z^J] + (z^J - z^I) \\ &\quad \{2(d-m+2dr-2r\gamma) - (z^J+z^I)(4r(d-m-r\gamma))\} \\ &= (z^J - z^I)\Bigg[\alpha[\sqrt{2}\cdot z^I + z^J]\left(\frac{\sqrt{2}\cdot z^I - z^J}{z^J - z^I}\right) + 2(d-m+2dr-2r\gamma) \\ &\quad - (z^J+z^I)(4r(d-m-r\gamma))\Bigg]\end{aligned}$$

Hence, the sign of Δ_{SC} depends on the term in squared brackets since from Proposition 3, we know that $z^J \geq z^I$. It can be shown that

$$\lim_{\alpha\to\infty}\Bigg[\alpha[\sqrt{2}\cdot z^I + z^J]\left(\frac{\sqrt{2}\cdot z^I - z^J}{z^J - z^I}\right) + 2(d - m + 2dr - 2r\gamma)$$
$$- (z^J + z^I)\,(4r(d - m - r\gamma))\Bigg]$$
$$= \frac{d^2(1 + 4r + 5r^2) - 2d(m + 2mr + 2r(1 + 3r)\gamma) + m(m + 4r\gamma)}{d - m + 3dr}$$
$$= \frac{f(d)}{d - m + 3dr}$$

where $f(d) = d^2(1 + 4r + 5r^2) - 2d(m + 2mr + 2r(1 + 3r)\gamma) + m(m + 4r\gamma)$, a quadratic in d with roots $\frac{2r(\gamma + m) + m + 6\gamma r^2 \pm r\sqrt{-m^2 + 4\gamma m(r + 1) + 4(\gamma + 3\gamma r)^2}}{1 + r(5r + 4)}$. The roots are real if and only if, $g(m) = -m^2 + 4m(1 + r)\gamma + 4(\gamma + 3r\gamma)^2 > 0$. Note that $g(0) > 0$, so f has real roots for m sufficiently small. Note also that $f(m) = mr^2(5m - 12\gamma)$ and $f'(m) = 2r(2m - 2\gamma + 5mr - 6r\gamma)$, so we have that

$$f(m) > 0 \Rightarrow 5m - 12\gamma > 0 \Rightarrow 2m - 2\gamma + 5mr - 6r\gamma > 2m - 2\gamma$$
$$+ 12r\gamma - 6r\gamma = 2m - 2\gamma + 6r\gamma$$
$$= 2m + 2\gamma(3r - 1) > 0 \Rightarrow f'(m) > 0,$$

where we have used the fact that $2r > 1$. This implies that $f(d)$ has at most one root d^* in the region $d > m$ because $f(m) > 0$ and $f'(m) < 0$ cannot hold simultaneously as shown above. Further, d^* exists if and only if $f(m) < 0 \Leftrightarrow m < \frac{12\gamma}{5}$ (i.e., m is small). Finally, if $d < d^*$ (i.e., d is small), then $f(d) < 0$. This proves the result. ■

References

Babich, V., & Tang, C. S. (2012). Managing opportunistic supplier product adulteration: Deferred payments, inspection, and combined mechanisms. *Manufacturing & Service Operations Management*, *14*(2), 301–314.

Babich, V., Burnetas, A. N., & Ritchken, P. H. (2007). Competition and diversification effects in supply chains with supplier default risk. *Manufacturing & Service Operations Management*, *9*(2), 123–146.

Caro, F., & Tang, C. S. (2014). Reducing collateral damages by imposing collective penalties. UCLA Anderson School Global Supply Chain Blog.

Caro, F., Chintapalli, P., Rajaram, K., & Tang, C. S. (2015). Improving supplier compliance through joint and shared audits. Unpublished manuscript, UCLA Anderson School, available at SSRN 2683515.

Caro, F., Chintapalli, P., Rajaram, K., & Tang, C. S. (2018). Improving supplier compliance through joint and shared audits with collective penalty. *Manufacturing & Service Operations Management*, *20*(2), 363–380.

Chopra, S., & Sodhi, M. S. (2004). Managing risk to avoid supply-chain breakdown. *MIT Sloan Management Review*.

Demick, B. (2013). Explosion at chinese auto parts factory kills 68, injured many more. Los Angeles Times.

Donaldson, T. (2014). Bangladesh resetting the bar on compliance standards. *The Sourcing Journal*.

Fuller, T., & Bradsher, K. (2013). Deadly collapse in cambodia renews safety concerns. New York Times.

Harsanyi, J. C. (1982a). Solutions for some bargaining games under the Harsanyi-Selten solution theory, part I: Theoretical preliminaries. *Mathematical Social Sciences*, *3*(2), 179–191.

Harsanyi, J. C. (1982b). Solutions for some bargaining games under the Harsanyi-Selten solution theory, part II: Analysis of specific bargaining games. *Mathematical Social Sciences*, *3*(3), 259–279.

Hendricks, K. B., & Singhal, V. R. (2005). An empirical analysis of the effect of supply chain disruptions on longrun stock price performance and equity risk of the firm. *Production and Operations Management*, *14*(1), 35–52.

Kapner, S., & Banjo, S. (2013). U.S. retailers near pact on bangladesh factory safety. *The Wall Street Journal*.

Kim, S. H. (2015). Time to come clean? disclosure and inspection policies for green production. *Operations Research*, *63*(1), 1–20.

Orsdemir, A., Hu, B., & Deshpande, V. (2015). Responsible sourcing via vertical integration and supply chain partnership. Working paper, UNC Chapel Hill Kenan-Flagler Business School, available at SSRN 2630733.

Plambeck, E. L., & Taylor, T. (2015). Supplier evasion of a buyer's audit: Implications for motivating compliance with labor and environmental standards. *To appear in Manufacturing & Service Operations Management*.

Rui, H., & Lai, G. (2015). Sourcing with deferred payment and inspection under supplier product adulteration risk. *Production and Operations Management*, *24*(6), 934–946.

Sodhi, M. S., & Tang, C.S. (2012). *Managing supply chain risk*, (Vol. 172). Springer Science: Business Media.

Sodhi, M. S., Son, B.-G., & Tang, C. S. (2012). Researchers' perspectives on supply chain risk management. *Production and Operations Management*, *21*(1), 1–13.

Tang, C. S. (2006). Perspectives in supply chain risk management. *International Journal of Production Economics*, *103*(2), 451–488.

Tang, C. S. (2013). Helping the poorest link in the chain: Bangladesh's garment factory workers. UCLA Anderson School Global Supply Chain Blog.

Tang, C. S., & Babich, V. (2014). Using social and economic incentives to discourage chinese suppliers from product adulteration. *Business Horizons*, *57*(4), 497–508.

Tomlin, B. (2006). On the value of mitigation and contingency strategies for managing supply chain disruption risks. *Management Science*, *52*(5), 639–657.

Van Mieghem, J. V. (1999). Coordinating investment, production, and subcontracting. *Management Science*, *45*(7), 954–971.

Wong, C. H., & Fung, E. (2015). More toxic goods stored near Tianjin homes. *The Wall Street Journal*.

Chapter 12
Leadership in Risky Supply Chains

Christopher R. Paparone and George L. Topic, Jr.

> Supply chains, once reliable assembly lines, are now spread across the globe and subject to constant, nonlinear disruption – everything from a food shortage in Zambia to a disease outbreak in China to a storm in the middle of the Pacific can impact delivery of a product packaged in the United States.
>
> General (US Army Retired) McChrystal et al. (2015: 249)

The essence of supply chain management is to make all the processes in the "chain" as smooth and predictable as possible; ironically, it is a critical task of leaders and managers to deal effectively with novelty,[1] anomalies, perturbations, and other risks to those chains. We believe this to be true universally within the discipline whether it is for the success of commercial entities, the provision of fulfillment services or—in our professional field—ensuring our national security. In the US Department of Defense and in other organizations worldwide and throughout history, the risks described below have been and will likely continue to be daunting.

The "logistics business" in the military is especially sensitive because of the constant pressure to minimize taxpayer cost—enabling the acquisition of more for less—while always being aware that the wartime risks of logistics failure can be catastrophic. There is a quote widely known in military circles attributed to Alexander the Great: "My logisticians are a humorless lot—they know if my campaign fails they are the first ones I shall slay." In modern militaries, the importance of military

[1] We define emergent as "novelty" as never experienced before in the organization's memory or having the unwelcomed surprise of an "emergency." In our view, dealing with novelty in supply chains is risky.

C. R. Paparone (✉)
Eisenhower School of National Security and Resource Strategy, National Defense University, Fort McNair, Washington, D.C., USA
e-mail: c.r.paparone.civ@ndu.edu

G. L. Topic, Jr.
Center for Joint and Strategic Logistics at Fort McNair, Washington, D.C., USA

G. A. Zsidisin and M. Henke (eds.), *Revisiting Supply Chain Risk*, Springer Series in Supply Chain Management 7, https://doi.org/10.1007/978-3-030-03813-7_12

supply chain management is similarly regarded as having risk to life and limb. Supply chain management within the Department of Defense, and by extension to the other parts of federal, state, and local government, intergovernmental organizations, and other nonprofit sectors differ in some ways from commercial enterprise; nevertheless, some fundamental *raisons d'être* remain when it comes to assuring supply fulfillment under risky conditions. In this chapter, we will offer some ideas about the importance of flexibility, agility, and creativity in leadership no matter what the sector.

The Honorable Alan Estevez, former Principal Deputy Under Secretary of Defense, often explained that military and commercial supply chains were very similar, with three significant differences: "First there was no "Christmas" season that came at a regular interval; second, we may not even know in advance when the equivalent of Christmas (for customer demands) will come and third, if we have a stock-out situation—for example with ammunition or fuel—there is a chance really bad things can happen" (personal correspondence with authors, January 2018). There are some additional considerations that make military supply chain operations different as well. In many cases, our customers are constantly on the move with no fixed address and in fact are trying to remain concealed. There are very few non-military enterprises where there are adversaries attempting to physically attack, interdict or destroy commercial supply chains (illegal narcotics distribution is one example) and of course, having the 535 members of the US Congress as your de facto "board of directors" introduces additional management challenges. All of these factors and many others make it pretty important that leadership in risky supply chains must encourage adaptation.

Two superb books on leadership that offer great insights on adaptivity are Ronald A. Heifetz's *Leadership Without Easy Answers* (1994) and his second book co-authored by Marty Linsky, *Leadership on the Line* (2002). These writers describe leadership as something different from exercising one's expertise in the face of the unexpected, that is, engaging in routine or "technical work." Their main idea is that leadership primarily occurs under emergent supply chain risky circumstances, where confusion on what to do coupled with the *social risks* of creative deviance represent the dangers of managing disruptive situations. Our purpose here is to extend this adaptive perspective into the context of leadership in risky, ever-changing supply chains. In lieu of well-engineered processes and adherence to repeatable techniques (standard operating procedures or SOPs) being the currency of effective work, we reorient on being creatively deviant as the most important aspect of the leader's work in the face of risky situations. Imaginatively influencing others to exercise divergent thinking and acting under unfamiliar conditions can be critical to adaptation.

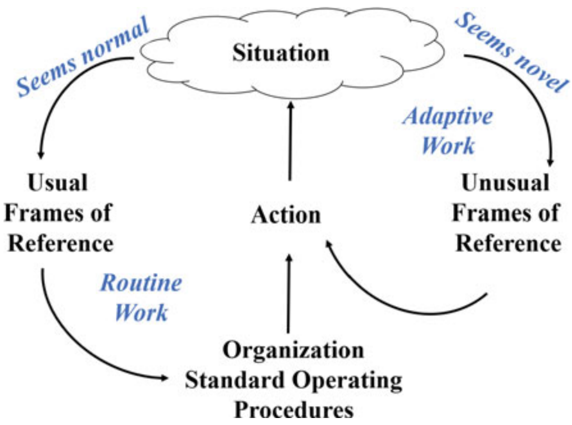
What we offer here are ideas on how to cope with emergent supply chain situations by reconceiving leadership as adaptive work that first requires an expectation that *what has worked well in the past may not work well now*. This can be a hard swallow as we have become accustomed to working in supply chains according to the proven SOPs across business functions in which we have learned to think and act with predictable results. Supply chain managers become technically proficient in business analytics, sourcing, transportation, warehousing, inventory management, risk management, and reverse logistics. Many operations managers pride themselves with detailed materials order planning, creating best practices, and controlling newly engineered processes that provide great efficiencies in manufacturing and services. Marketing specialists attend to the art and science of consumer psychology, pop culture, demographic trends, and leverage an expanding array of mass and targeted communications media. Human resource experts bring their techniques of labor law interpretations, approaches to talent management, enforcement of occupational safety, equal employment opportunity, and diplomacy in workforce relations. Finance and accounting professionals specialize in the disciplines of business economics, audits, tax law, loans, and investments and so forth. We are by no means disparaging these highly honed and important competencies that guide professional practice; rather, we are arguing that exercising these time-tested techniques should not be the only foci of supply chain management expertise. The focus of adaptive work—leading divergence in the face of emergent disruptive situations in supply chains—is of at least equal importance, and, in the military context, may mean the difference between winning and losing a battle or war.

The precision of practiced routinized practice is thus juxtaposed with the need for creative divergence in managing supply chain operations. The difference lies in how we collectively *frame* situations—between employing our confirmed, reliable frames of reference and recognizing those that require reframing. When faced with stable situations, we can rely on our training and organizational knowledge that works much like our own "memory" becomes second nature in action; that is, we employ the *usual* frames of reference. We tend to orient action based on the familiarity of known-knowns or what Heifetz calls "technical work"—doing things which have worked well in the past. On the other hand, risky situations require adaptive work, taking transformative approaches that are radically different. Leadership seeks to influence others to create *unique* frames of reference while acting in and reflecting on novel situations. Figure 1 is a model of how tried and true routine (usual) and adaptive (unusual) efforts work in tandem. The more novel the emergent situation, the more divergence should take hold as we realize standardized frames of reference will not work under unfamiliar conditions.

1 Dropping Old Tools

Abraham Maslow coined the proverbial tool metaphor: "I suppose it is tempting, if the only tool you have is a hammer, to treat everything as if it were a nail" (1966, p. 15); this shibboleth is used often when critically examining aspects of military supply chain, emergent risk, and decisions about what to do about it. The supply chain leader helps others search for unusual frames of reference in the context of the unfamiliar, purposefully avoiding the organizationally accepted frames that would try and "hammer" the situation into something more familiar. Adaptive leadership pursues unusual frames of reference finding new meanings in situations through the artful and improvisational creation of new frames of reference. Rather than belief in the superiority of organizationally accepted technical competencies (signified by the

Fig. 1 Routine with respect to adaptive work is situationally dependent



learning loop on the left side of Fig. 1), practice in novel situations should be recast as a matter of deviation from normal practice (the learning loop on the right side of Fig. 1). That is not to say that past reported inquiries and theories that do not work now should be discarded; rather, that they may be at least temporarily displaced by more improvisational or innovative meanings for action that addresses the moment of confusion. Donald A. Schön, philosopher and professor of urban planning at the Massachusetts Institute of Technology, put it this way:

> The nonroutine situations of practice are at least partly indeterminate and must somehow be made coherent. Skillful practitioners learn to conduct frame experiments in which they impose a kind of coherence on messy situations and thereby discover consequences and implications of their chosen frames. From time to time, their efforts to give order to a situation provoke unexpected outcomes – "back talk" that gives the situation a new meaning (1987: 157–158).

Furthermore, Schön points out that knowledge-at-work has to become malleable and inventive:

> …if you are dealing with a unique situation, then by definition you cannot apply to it standard categories of analysis and action. Because if it's unique, just that about it which is unique does not fit those categories. And therefore, you have to do something on the spot in such a situation, something that involves invention, which involves reconfiguring the problem, which may involve redesigning categories so that they fit it. (1995: 239).

The focus of supply chain leadership, then, would be to coach and participate with stakeholders' critical and creative conversation about the confusing situation at hand. As such, the adaptive leader promotes deep, artful, critical, and interpretive excursions into others' divergent frames of reference and creative departures from that past organizational learning ultimately designing new frames of reference. In his later work, Schön, co-authored with Martin Rein, the process of reframing stands in critical opposition to the existing "underlying structures of belief, perception, and appreciation" that have been institutionalized (1994, p. 23). Hence, reframing involves a purposeful attempt to interrupt the shared, normalized ways of making sense of emergent, risky situations.

The innovative design of unusual frames of reference when faced with novel situations involves bringing the confusing world into mixed thought trials or "frame experiments." The group, led by the adaptive leader, may also practice real-time trials in the midst of confusing situations. Such conversations and actions in the fog of confusion should not be tightly governed by conventional approaches (i.e., Maslow's "hammer") that may dangerously provide the illusion of understanding (everything is a "nail"); rather, be more fluid, where practitioners become actively immersed, imaginative, and mindful in making new sense (emphasis added, Schön 1995: 389). These conversations should be expected to be "complex, defamiliarizing, rich in paradox," hence, "…clearing away conventional notions to make way for artful and exciting insights" (DiMaggio 1995: 391).

The insights of Heifetz, Linsky, Schön, Rein, and others that built on their work, can be applied to almost every disruptive situation; their ideas for generating creative approaches to complex problems have given rise to several models from both academic institutions and practitioners. In the realm of supply chain management, these ideas are especially useful and important, as the constantly changing nature of markets, global competition, and the speed of electronic commerce all require continuous assessment and rapid adaptation. Organizations that cling mindlessly to a regimented business practice, that have proved successful in the past need to recognize that their very existence is at risk—and they often recognize it too late. In supply chain management, there is a constant struggle between the presumed more efficient routine, standardized process and the more innovative solution—the reframing that Professor Schön highlights—is fighting disruption with disruptive reframing and may even be more expensive in the short term. Obviously, the best supply chain leaders are those that can lead reframing efforts and quickly adapt supply chain organizations and processes to meet emergent risk. While there may be countless more, we offer two models for supply chain leadership that will stimulate creative and inventive frames of reference for risky circumstances: *Reframing through Divergence* and through *Reframing Value Patterns*.

2 Reframing Through Divergence

> The system removes the threat of anyone exercising their independent will. Divergents threaten that system. It won't be safe until they're removed.
>
> —Jeanine Matthews[2]

The first model, divergence, seeks to increase inter-organizational and interpersonal diversity in the team which has been charged with dealing with the emergent risk

---

[2]Jeanine Matthews was the antagonist character in the 2014 movie *Divergent* © played by Kate Winslet.

at hand. The leader sets conditions for others to pursue a new pathway while constructing a new sense of the reality they are facing along the way. One person's usual frame of reference is another's unusual frame of reference; whereas, together, they may work in tandem as an entirely innovative approach to a novel situation.

We are reminded of the popular trilogy science fiction novels (Roth 2013) and Summit Entertainment movies, *Divergent*, presenting a world where people are tested and separated to live and work with like-minded others, each group bringing their distinct way of constructing reality together to form a balanced and stable society. The appearance of the divergent insurgents (i.e., those who can create a new societal reality) who see conflict over whose perspective is best is not something to be suppressed but serve as the source of inventive management and the creation of more dynamic and exciting ways to deal with complex societal issues.

As the movie portrays, the utopian "high-performing team," where frames of reference are shared in a mutually trusting, well-balanced, and egalitarian fashion, is not only very difficult to achieve, but may be contrary to the idea of adaptive work. The goal of divergence is to emancipate and give voice to opposing (i.e., not necessarily complementary) frames of reference—embracing how each member interprets the novel situation differently. After all, situations do not transmit meaning in and of themselves; humans place meaning on them. That meaning is based in frames of reference that include traditional knowledge disciplines, family upbringing, schooling, personality preferences, and unique cultural perspectives. Management here is based in giving voice and finding ways to protect against those who have such divergent views that they are scoffed, socially excommunicated, or at the least, not taken seriously.

As an exemplar, the US Army has invested in an institution called the University of Foreign Military and Cultural Studies (UFMCS 2017) which provides handbooks, guides, and articles seeking ways to give voice to divergent views—the Army calls the opposition process "red teaming." The UFMCS faculty is specially trained in anonymity techniques, positive engagement methods, "taking the rank off at the door," and so forth, practices all geared to removing barriers to getting divergent ideas on the table. The UFMCS offers three types of activities that the leaders may employ to facilitate divergence:

(1) *Increasing cross-cultural empathy*—methods include Multi-framing, "4-ways of seeing" exercises, and storytelling in cultures (narratology);
(2) *Rewarding introspection and critical reflection*—includes exposing institutional assumptions and beliefs and conducting "pre-mortem analysis"—envisioning what failure may look like; and,
(3) *Mitigating groupthink*—approaches to minimize the blinders of extreme, unreflective consensus.

All of these methods address social barriers by exposing red herrings (e.g., fear of powerful bosses and dominating people who coerce subordinates or coworkers to use organizationally accepted competencies regardless how novel the situation seems—these amount to fallacious appeals to authority or submission to organizational "power politics"); and, preventing clan-like cultural habits (e.g., valuing "the team" more than the tough decisions; and, the self-censoring correlated to the importance of the decision—that is, fear of speaking up as your idea may be tried; hence, you are to blame if the idea fails). One can access the UFMCS handbooks online in the public domain. We encourage the aspiring adaptive leader to try some of the anonymity methods at work or at home. These red teaming methods of divergence permit ideas to get on the table with the protection afforded by anonymity. While these may help get ad hoc groups started in getting different ideas out in the open by minimizing the social barriers normally encountered, there may still be a requirement for reframing value patterns.

3 Reframing Value Patterns

The essence of supply chain management and frankly for leadership in general is in fact navigating a plethora of paradoxes—evaluating relative trade-offs, making decisions and effectively implementing action once a decision is made. Inevitably and naturally, any option for prioritization is going to come at the cost of an alternate approach—and likely proponents or stakeholders who will promote what seems best from their perspective. The essential factor in this process is being able to frame or value various options against the core purpose and/or objectives of the organization—and this is true for all supply chains from the most simple to the most complex and whatever the nature of an enterprise might be, commercial, military or others such as NGOs, humanitarian organizations, etc.

To restate the problem, we are addressing divergence from an existing set of organizationally accepted values that have been inculcated into its members. The need for adaptive and creative revaluations in the face of emergent supply chain risk becomes obvious. It is a strange paradox that the reliability of subordinates to accomplish the tasks and missions they are assigned in the "right way" often determines who gets promoted; yet, in a highly structured command and control hierarchy, such as the military, the skills needed for the successful senior ranking logistician are not often prized or rewarded in junior officers or young civilian Defense Department supply chain managers. In fact, such deviant revaluations can be quite dangerous to career progression. The bottom line is that one of the most important values for action in both military and commercial organizations that undergirds leadership in risky supply chain management is not conformance, but creative deviance. And this skill requires the ability to step away from the familiar and well-understood and examine an environment, as Paul DiMaggio noted, that is "complex, defamiliarizing and rich in paradox" (1995: 391). Novel situations, requiring adaptive leadership, may call for defying institutionalized valuations and require what we would call *paradoxical interpretation* (based in the work of Cameron and Quinn 1999).

How does one go about shifting from the preference for an accepted institutionalized value-pattern to an opposing value-pattern? While supply chain professionals may be oriented on *process control* as a dominant value frame for what the institution was designed to upkeep, re-patterning would require them to seek a contrasting value

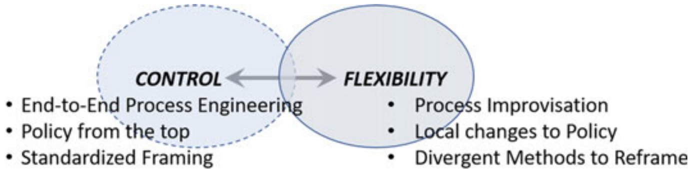


Fig. 2 Opposing values of control with respect to flexibility in supply chain. The solid-lined oval represents the organizations normalized frames of reference that work under normal conditions. The dotted-lined oval reflects a shift because of the needed re-patterning of values

to consider other ways of appreciating the messy supply chain situation at hand. For example, a paradoxical value to process control is *process flexibility*. The more control that management seeks (such as engineering highly efficient processes), the more the people that work there may feel their ideas for change are stifled (i.e., they are not at liberty to flex processes when unfamiliar conditions dictate). Figure 2 portrays the necessary reframing or re-patterning of values, in this case flexibility with respect to control.

Logistics executives and senior officers across the Department of Defense reflexively seek tighter control over supply chains by invoking the reengineered of processes from "end to end;" that is, developing a detailed supply chain architecture from manufacturing, through distribution, all the way to the point of consumption. We have purchased expensive commercial information systems to achieve better financial accountability and efficiencies associated with managing billions of dollars in military hardware (repair parts, ammunition, etc.). While managing the massive supply chain through a host of automated control measures, we also must consider the downside of achieving "Lean and Six Sigma" style efficiency with our logistics systems (Paparone 2008). To deal with an uncertain supply chain in the fog of war, we recognize that logisticians working in national depots as well as in fighting units must be developed to be adaptive leaders. This desired adaptive work is associated with a required value shift creating flexibility in otherwise tightly controlled supply chain activities to deal with interruptive surprises that put the lives of soldiers, sailors, marines, and airmen at risk. The value shift from control to flexibility can apply to all supply chains that are subject to unforeseen novelty; hence, empowering adaptive leadership all along the supply chain is required. Shifting the value from one side to another becomes more like playing music along a continuum—from the directed music of an orchestra and single designated conductor to that of an improvisational jazz band where the lead shifts among the artists.

Another challenging paradox at work in supply chain management involves a supply chain *collaborative* belief system among members with respect to a supply chain *competitive* belief system of each enterprise member (Fig. 3) (Clarke-Hill et al. 2003). The tension between these poles with affiliates in a supply chain is apparent with the sharing of information, which may be proprietary and is often of great value to the owning company but at the same time may help others in the value chain make

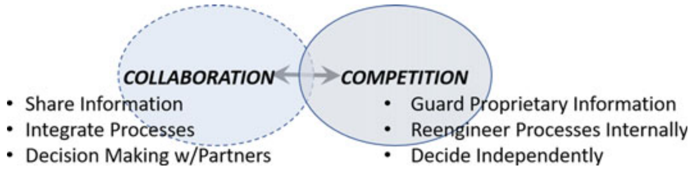


Fig. 3 Opposing values of collaboration with respect to competition in supply chain

the overall system work better. This is the central lesson of the iconic "Beer Game" that virtually every entry-level supply chain student gets to simulate in some form.

For many companies, intellectual property is their crown jewel and constitutes the difference between thriving with a distinct competitive advantage and literally ceasing to exist. It is important to understand that intellectual property is not always a secret recipe or electronic invention but may be a key process design that constitutes a competitive advantage. For example, in the extremely fast-moving world of women's clothing cutting a few days off the time-to-market can significantly affect profit margins. Innovative processes to assemble and distribute products are a major focus of leading companies around the world—and of course in an increasingly global marketplace this is even more important. But of course, supply chain management requires sharing information, integrating processes, and collaborative decision making with external members across the supply chain. Leaders at all levels are continually faced with challenging decisions to manage the tension between the risks of collectivism with the risks of individualism.

There are many other types of opposing values that leaders of all types face at every level throughout their careers. Simplicity with respect to complexity, data-driven risk analysis wrt intuition, tradition wrt innovation are but a few more continua of "opposite values" that require continuous searching for the best balance between poles. As with everything else discussed in this chapter, the ability to see and understand the internal working of one's organization with respect to the external environment (the others in the chain) and the agility to respond with appropriate speed to both are the keys to success. To initiate reframing associated with opposing values is to notice when a "pattern shift" is needed—revaluation and balance are key considerations of the supply chain leader. However, as the leader initiates and encourages divergence, revaluation, and rebalancing, they may experience other challenges or unforeseeable consequences.

4 The Hazards of Adaptive Leadership in Dynamic Supply Chains

> … every day you must decide whether to put your contribution out there, or keep it to yourself to avoid upsetting anyone, and get through another day. You are right to be cautious. Prudence is a virtue. You disturb people when you take unpopular initiatives in your community, put

> provocative new ideas on the table in your organization, question the gap between colleagues' values and behavior, or ask [others]to face up to tough realities. You risk people's ire and make yourself vulnerable. Exercising [adaptive] leadership can get you in a lot of trouble.
>
> —Ron Heifetz & Marty Linsky (2002, p. 2)

Leading group reframing excursions is not easy, particularly from being seen as a rogue or deviant participant (which is why we strongly recommend the anonymity techniques espoused and taught by UFMCS). Heifetz explains adaptive work:

> Rather than fulfilling the expectation for answers, one provides questions; rather than protecting people from outside threat, one lets people feel the threat in order to stimulate adaptation; instead of orienting people to their current roles, one distorts people so that new role relationships develop; rather than quelling conflict, one generates it; instead of maintaining norms, one challenges them (1994: 126).

Such heretical-style leadership is messy, eclectic, interactive, inventive, politically dangerous (in the military and law enforcement context, perhaps physically dangerous), technically unstructurable, countercultural, institutionally deviant, risky, hypothetical, and may end up endangering the career advancement or even continued employment of those exercising it. Small deviations from the norm (a.k.a. organizationally accepted values) challenge those in power who may see such deviations as arrogant and disrespectful as they identify themselves with the organization's way of doing things—after all, that's how they were successful and moved up the hierarchy. Accepting a countervailing narrative may result in loss of power; hence, destabilizing the "sacred" values and power structure of one's workplace even though an enterprise working group may find or want to test an approach that is unconventional to any of their home institutions.

Heifetz and Linsky (2002) offer advice to deal with this social risk in part two of their book. We offer a few synopses to give you a flavor:

- "Get on the balcony:" Try to place yourself outside the problem space to have a different perspective (this is the essence of reframing and revaluing).
- "Think politically:" build relationships and deal with those who have strong opposition to reframing and revaluing.
- "Orchestrate the conflict:" maybe through a professional, unbiased facilitator (like the "red teamers" at UFMCS) or a neutral physical location.
- "Give the work back:" make the issue your responsibility until solved while transferring much of the reframing and revaluation work to others.
- "Hold steady:" there will be accusations and pressures to back down, especially as you are suggesting the organizational frames and values must change.
- "Manage your stress:" meaning, manage your anxiety even when you don't feel it.
- "Anchor yourself:" relationships outside of work (like family) are lifelong importance, remember there is life after this role is completed and you need that support. (pp. 51–206)

Heifetzian style leadership is challenging, by definition fraught with risk, and not for everybody. That said there is risk in inaction as well as strictly adhering to long-standing or well-established practices. We recognize such responsibility and acceptance of career risk associated with creative deviance too stressful or disconcerting for many people and their institutions. Such leadership is not for the faint of heart.

5 Conclusion

As Abraham Lincoln famously said: "The dogmas of the quiet past are inadequate to the stormy present. The occasion is piled high with difficulty, and we must rise with the occasion. As our case is new, so we must think anew and act anew." We found it difficult to present a deep case proposing the case for leadership in risky supply chains in a single book chapter. The emergent supply chain circumstances we continuously face in the Defense Department are often unusual and facing emergent risk in any context requires unusual ways to reframe and revalue. Our organizationally accepted technical competencies, which we rightfully pride ourselves as "experts" will likely not work well in dealing with emergent risk in supply chains.

Heifetzian leadership requires uncommon reframing and revaluations in dealing with unusual situations. In both national security and commercial realms, we need to develop leaders that are critical of the ways we have been taught to act in familiar situations and seek ways to respond to the unfamiliar. It is also important to recognize that one should not be naïve when choosing to take this more socially dangerous path of adaptive leadership. We hope that we have at least whet the reader's appetite and provided motivation to dig deeper into our reference list that follows. These are marvelous resources for the lifelong learner interested in honing his/her skills in managing risky supply chains—requiring leadership that leads creative deviance as the "new norm."

Disclaimer The views expressed are the authors' and do not necessarily reflect the official policy or position of the National Defense University, the US Department of Defense or the US Government.

References

Cameron, K., & Quinn, R. E. (1999). *Diagnosing and changing organizational culture*. Reading, MA: Addison-Wesley.

Clarke-Hill, C., Li, H., & Davies, B. (2003). The paradox of co-operation and competition in strategic alliances: Towards a multi-paradigm approach. *Management Research News, 26*(1), 1–20.

DiMaggio, P. J. (1995). Comments on "What theory is not". *Administrative Science Quarterly, 40*(3), 391–397.

Heifetz, R. A. (1994). *Leadership without easy answers*. Harvard: Harvard University Press.

Heifetz, R. A., & Linksy, M. (2002). *Leadership on the line: Staying alive through the dangers of leading*. Boston: Harvard Business School.

Maslow, A. H. (1966). *The psychology of science: A reconnaissance*. New York: Harper & Row.

McChrystal, G. S., Tantum, C., Silverman, D., & Fussell, C. (2015). *Team of teams: New rules of engagement for a complex world*. New York: Penguin.

Paparone, C. R. (2008). A values-based critique of lean and six sigma as a management ideology. *Army Logistician, 40*(1), 34–40.

Roth, V. (2013). *Divergent trilogy*. UK: HarperCollins.

Schön, D. A. (1987). *Educating the reflective practitioner*. San Francisco, CA: Jossey-Bass.

Schön, D. A. (1995). Educating the reflective legal practitioner. *Clinical Law Review, 2,* 231–250.

Schön, D. A., & Rein, M. (1994). *Frame reflection: Toward the resolution of intractable policy controversies*. New York: Basics Books.

UFMCS (2017). University of Foreign Military and Cultural Studies information. Retrieved August 25, 2017, from http://usacac.army.mil/organizations/ufmcs-red-teaming.

Chapter 13
Malicious Supply Chain Risk: A Literature Review and Future Directions

Scott DuHadway and Steven Carnovale

1 Introduction

Managing supply chain risk is an important component of supply chain management and is generally defined as "the likelihood of an adverse and unexpected event that can occur and either directly or indirectly result in a supply chain disruption" (Garvey et al. 2015, p. 619). Risks can vary from major disruptions due to natural disasters, supplier bankruptcy, quality failures, fraud, etc. In order for firms to develop a resilient supply chain, it is important that they are able to correctly interpret supply chain risk and adapt operations to meet those risks (Ambulkar et al. 2015; Pettit et al. 2016). Thus, research in this area has explored much in terms of how to effectively manage risks that are, implicitly, from inadvertent causes such as weather-based disruptions or accidental supply failures through a variety of process-focused (i.e., procedural recommendations/techniques to mitigate risk) research. However, much opportunity remains to explore the role of relational risk associated with other companies or individuals in the supply chain engaging in malicious behaviors that can lead to disruptions. With that in mind, it is important that researchers recognize a type of risk that has received limited attention in the literature, which we identify as malicious supply chain risk. We define malicious supply chain risk as the risk a firm has as a result of an individual or organization making a deliberate decision that can lead to harmful outcomes on the firm and its extended supply chain. Examining *malicious risk and disruptions* is worthwhile, considering how relatively unexplored they are. Accordingly, the following sections will explore these areas in detail.

S. Carnovale (✉)
Saunders College of Business, Rochester Institute of Technology, Rochester, USA
e-mail: scarnovale@saunders.rit.edu

S. DuHadway
Portland State University, Portland, OR, USA
e-mail: duhadway@pdx.edu

G. A. Zsidisin and M. Henke (eds.), *Revisiting Supply Chain Risk*, Springer Series in Supply Chain Management 7, https://doi.org/10.1007/978-3-030-03813-7_13

2 Literature Review

Though this area has received little attention, we note that the research on risks associated with malicious behavior has been increasing over the past few years. The evidence suggests that companies are increasingly facing crises from product harm that results in a product recall (Liu et al. 2017). Despite these increases, there is limited research which explores the motivation to engage in fraudulent actions at an organizational level (Arnold et al. 2012). For example, some studies have explored aspects of disruption risk related to intentional behavior in some way, including threats from theft, piracy, terrorism, contamination, counterfeiting, and product tampering (McGreevy and Harrop 2015), preparing a supply chain for premeditated attacks on facilities (Parajuli et al. 2017), how to monitor fraud risks in the supply chain (Vollmer 2015), and issues related from profiting from product-harm crises in competitive markets (Rubel 2018), among others.

While much of the research in this area explores specific threats/risks, there is some research that advances strategies for managing these types of risk. DuHadway et al. (2017) explore key differences in how to manage intentional disruptions (similar to the concept of malicious risks defined in this chapter) as opposed to traditional disruptions, suggesting that mitigating intentional disruptions requires relationship-based approaches, while recovering from disruptions requires the ability to restructure a supply chain. Other research suggests that manufacturers must build forms of relational governance to safeguard against the relational risk of partners (Cheng and Chen 2016). Additionally, research which identifies the antecedents of similar (malicious) disruptions or opportunistic events has found that power asymmetry/imbalance culture can lead to malicious risks (Villena and Craighead 2017; Madichie and Yamoah 2017).

Perhaps, the literature stream most closely connected to malicious risks is that which explores opportunism, or "self-interest seeking with guile" (Williamson 1985). Opportunism is often thought of as the calculated efforts of an exchange agent to mislead or otherwise obfuscate, or distort, a transaction (Williamson 1985). Perhaps, a more applicable way to frame the impact of opportunism, particularly as it relates to malicious risks, can be described as a partner within an exchange relationship not acting in the best interests of the opposing partner (Doney and Cannon 1997). In this case, there is a breakdown of trust in the relationship. Trust is typically broken down into two critical constructs: credibility and benevolence (Morgan and Hunt 1994; Doney and Cannon 1997; Ganesan and Hess 1997; Huang et al. 2008; Suh and Houston 2010). Credibility is the belief that the supplier will fulfill its promises while being reliable and consistent in its commitments (Dwyer et al. 1987; Morgan and Hunt 1994; Ganesan and Hess 1997). Credibility, with respect to the supply chain literature, is a critical component to relational exchange (Ganesan and Hess 1997). Benevolence is the belief that a partner in an exchange relationship will not act opportunistically if given the chance (Doney and Cannon 1997; Ganesan and Hess 1997). Researchers have given serious emphasis to the development, formation, and management of trust. Given this emphasis, trust is a fundamental underpinning for

Fig. 1 Examples of malicious and traditional risks. Adapted from DuHadway et al. (2017)

the development of the working dynamics between firms. Using opportunism as a basis, we can identify several behaviors that fit with malicious risk and that have seen some exposure in the literature (Fig. 1).

2.1 Examples of Malicious Risks

Consider the two major automotive recalls of Takata air bags and the Volkswagen emissions scandal. The Takata airbag recall, which was the largest automotive recall in history, occurred because Takata switched their production to using ammonium nitrate instead of tetrazole in their airbag design to cut costs and then lied to their customers regarding the safety of the new compound being used (Trudell et al. 2014; Trudell and Fisk 2016). Takata "routinely manipulated results of airbag inflator tests" (Trudell and Fisk 2016). Data indicating the risk of the air bags was deleted, and customers were unaware of the risks that Takata knew and understood. Takata engaged in malicious behavior to advance their interests at the expense of their supply chain partners.

Volkswagen engaged in deceptive practices which ultimately led to a recall for their vehicles which used software to deliberately cheat emissions testing, causing an estimated 59 premature deaths (Barrett et al. 2015), and a financial settlement of over $15 billion in the USA (Fisk et al. 2016). Interestingly, in both of these cases safeguards were in place (airbag inflator tests to verify safety and the emissions testing procedures) to prevent problematic behavior, yet the firms intentionally circumvented such process controls and engaged in malicious behavior for their own self-interest.

In 2013, it was found that beef lasagna contained horsemeat of varying percentages, with some of them containing 100% horsemeat (Brown 2013). It is challenging to think that the introduction of horsemeat into the beef supply chain occurred through some inadvertent or accidental measure, particularly given that differentiating between a horse and a cow is rather simple. At some point in the supply chain, someone made the decision to substitute a horse for a cow and sell it as beef and did so intentionally, likely because it saved them money. Even though beef and horsemeat might be reasonably comparable, the act of deception in the supply chain is what serves to motivate the exploration into malicious risks. If our supplier says, "This is beef"—should we not be able to rely on that statement? And if we do decide that we are not ready to trust our supplier, how can we protect ourselves from when suppliers decide to deliberately deceive us, or when our suppliers themselves have been duped? The issue of product deception and fraud very quickly becomes a supply chain issue, particularly because the ramifications of deceptive behavior have far-reaching effects on all members in the supply chain.

There are examples of firms who have taken the appropriate quality control measures to protect their supply chain who have been impacted by deliberate deception of a supplier. The lead-based paint toy recalls from 2007 which Mattel experienced are notable because Mattel established and paid for a testing facility, thus taking what would normally be appropriate measures to ensure that the materials coming into the supplier's facility were of appropriate quality. However, their supplier intentionally avoided the testing facility (Woo 2008). Accordingly, we need to rethink the way we manage a supply chain to limit our exposure to malicious risks. Traditional process-based approaches can be ignored or circumvented.

Malicious risks can take a variety of different forms, including falsifying data, supply chain fraud, counterfeit manufacturing, digital security threats, intellectual property theft, contract breach. A 2012 study found that 33% of the 1215 fish samples collected at restaurants, sushi vendors, and grocery stores were labeled incorrectly (Warner et al. 2013). Supply chain fraud has been identified as the "single most exposed area" of fraud (Bhide 2012, p. 16). Counterfeit manufacturing has become a large problem in the automotive supply chain, and examples of their impact on manufacturers and consumers are not difficult to find. Daimler seized 1.6 million counterfeit products in a single year (Daimler 2017). Mislabelled counterfeit plastic parts in Aston Martin vehicles have led to major recalls (Wowak and Boone 2015; DuHadway et al. 2017).

Much of the research on supply chain disruptions has explored it from the perspective of managing it via process-based controls. For example, research on automotive recalls has explored it from a process-based view (Shah et al. 2017), but there is evidence of a number of recalls which happened even though "specific measures were undertaken by the firms to avoid such issues," suggesting that "efforts to improve quality performance of vendors may not be effective" (Agrawal and Muthulingam 2015, p. 350). So, how then should we manage these types of risks? Some strategies involve different approaches. For example, Babich and Tang (2012) suggest deferred payment outperforms inspections as a more effective way to eliminate opportunism such as product adulteration.

If we are relying on process-based controls, we are inherently relying on trust as a protection mechanism to ensure that such procedures are followed. While trust can be good, consider the dark side of trust as well. To highlight this dark side of trust, consider the example provided in the book *Turtles of the World* (Bonin et al. 2006). The authors explore a number of different species of tortoises, finding that in some species an interesting symbiotic relationship emerges between the turtles and some local finches. The finches eat the small bugs and parasites that live on the turtles, particularly in hard to reach places such as under the head and neck of the turtle. This behavior involves a turtle signaling to the bird by raising up on its front legs and letting the bird crawl underneath him to eat the insects. However, some of the turtles have tasted the dark side and learned that by suddenly dropping itself onto the bird, it can catch the bird under its shell, crushing it and providing a good source of nourishment in the form of newly tenderized protein. Although this example is quite extreme, trust in relationships is exhibited in similar ways. It slowly develops over time as expected behaviors emerge which can form mutually beneficial relationships. Yet, if one party decides to start playing unfairly, it can have dramatic consequences on the other involved parties.

3 Managing Malicious Risks

We explore three traditional approaches for managing risk: detection/avoidance, mitigation, and recovery. These three phases of risk management represent before, during, and after a disruptive event has occurred (Fig. 2).

Detection can serve as an early warning system or can help to dodge a disruption completely. If the disruption is unavoidable, it can ensure that good plans are in place to manage the disruption once it occurs. For example, take the recent example of bitcoin's price volatility (Sapuric and Kokkinaki 2014). Such fluctuations in price have led to shortages of video cards and incredibly high prices, as one of the ways that bitcoins can be gathered is through electronic mining which is most efficient using high-end graphics cards. However, due to the fluctuation of prices of bitcoins, the demand is highly uncertain and difficult to predict. Being able to observe early market trends can help firms avoid underproducing or over-producing products leading to either a disruption or a surplus of product that needs to be liquidated at a lower price.

A number of detection and avoidance mechanisms exist, including quality management (Lee and Whang 2005), information sharing (Sheffi 2001; Kleindorfer and Saad 2005), supplier audits and supplier development (Giunipero and Eltantawy 2004), and security assessment and management practices (Finch 2004). Even though there are many different mechanisms for detection, effective detection which comes from information sharing, supply chain visibility, and supplier integration can detect or prevent a variety of disruptions (DuHadway et al. 2017). Another effective mechanism to limit malicious risks is transparency. For example, blockchains have been suggested as a potential avenue for increasing transparency with smart contracts

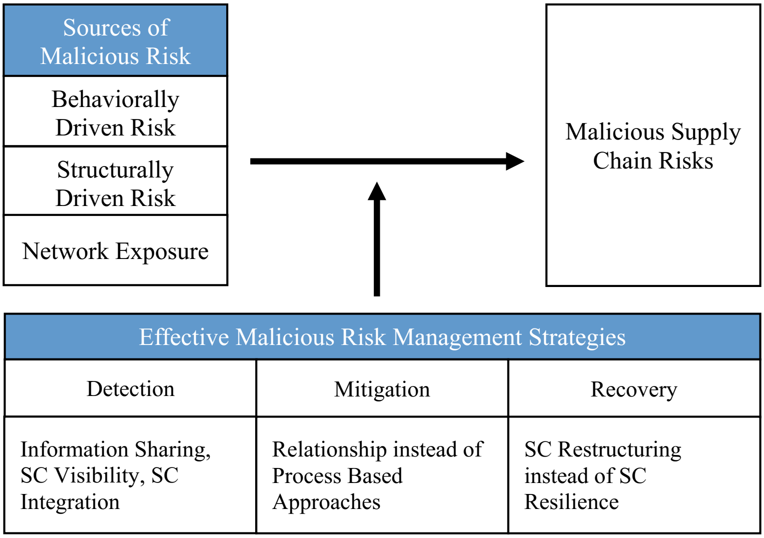


Fig. 2 Sources and mitigation strategies for malicious risks. Adapted from DuHadway et al. (2017)

(Nugent et al. 2016). Further research into the area of technology tools to enable transparency is necessary so as to provide recommendations in this area, however.

Mitigation can limit the potential impact of a disruption occurring. This is critical for minimizing the harm to a supply chain from a disruption. Some research suggests that structural approaches can help to mitigate damage, such as modularity and diversification (Kleindorfer and Saad 2005). Other more traditional approaches might include stockpiling inventory (Chopra and Sodhi 2004; Tomlin 2006). These strategies are important to recognize, because it is possible that these strategies exacerbate the risks of malicious disruptions rather than limiting them. For example, consider the impact of high levels of inventory when the disruption is due to supply chain fraud such as lead-based paint in children's toys. Higher levels of inventory would then need to be discarded in addition to the carrying costs of maintaining higher levels of inventory. Modularity has been argued to generally limit exposure to opportunism (Lippman and Rumelt 1982; Pil and Cohen 2006), but if the modular system is compromised through intellectual property theft or counterfeiting, the issue could be further exacerbated because the entire system is now compromised.

Recovery is another aspect of risk management that requires a completely different approach. One of the most common approaches for risk recovery is to develop a resilient supply chain, or one that is quickly able to return to its previous state after a disruption (Christopher and Lee 2004). However, this approach is counterintuitive when the disruption is caused by malicious risk. When the disruption is caused by malicious risk (i.e., finding out that your supplier has been selling you a counterfeit product), there is no value in returning to the previous state, so resilience-based recovery approaches are insufficient. Using an analogy of a human immune system, we can liken resilience to being able to recover from injury. Such injuries generally occur from an external cause, and the goal of recovery is to return to full functionality from the injury. However, disruptions from malicious risks could be seen as analogous to symptoms of an infectious disease. In such a case, it might require addressing the conditions that led to the symptoms internally. Without treatment, the infection could significantly worsen and lead to other problems. The goal should not be focused only on treating the symptoms, but the core of the problem. In extreme cases, it might require removal of the infected part. The approach that should be taken when a supplier has a product quality failure due to some accidental cause should be substantially different than when a supplier intentionally deceives or lies about product quality and intentionally substitutes an inferior product to make money. Recovering from malicious risks will require a more substantive approach which will require restructuring the supply chain, for example, by excising the supplier, or more fundamental approaches to addressing the cause of the disruption. Appropriate supplier relationship management could help substantively in this area.

4 Drivers of Malicious Risks

The above discussion makes clear that dealing with malicious risk through the prism of traditional supply chain risk management can be insufficient for preventing disruptions due to such risks. The reason is that the causes for the manifestation of such risks are different, and so too are the impacts that they have on the network in which the firm is embedded. Although the research on malicious risks is relatively limited, we propose that the drivers (i.e. antecedents) of such malicious risks can arise from three core areas: (1) the microlevel: behavioral drivers; (2) the mesolevel: structural drivers; and (3) the macrolevel: network exposure as a driver. Below, we briefly explore the implications of each of these drivers and propose a research question motivating each area's future work.

4.1 Micro-Drivers: Behaviorally Driven Risk

Take the example of the fraudulent beef lasagna example above, where at one point someone made the choice to swap horse for beef and include it in the supply chain. This is a microlevel decision with cascading impacts on the rest of the supply chain. Concepts such as dependence asymmetry, trust and relational governance, transitive trust, cultural norms and values, business ethics can provide interesting insight into terms of how we can limit malicious supply chain risks. At this level, a core research question is: *What relational mechanisms engender the development of malicious supply chain risks?*

4.2 Meso-Drivers: Structurally Driven Risk

The structural drivers of malicious risk can include risks associated with the general trends to the changing environmental conditions surrounding supply chain management in a modern era. These include the increasing reliance on digital manufacturing, high levels of modularity, data security processes, the world becoming increasingly connected, and emergent cultural differences through a more connected world. Take, for example, the recent ascendency of blockchain technology into various supply chain processes. On the one hand, it promises increased transparency and visibility (Nugent et al. 2016), yet in order for the supply chain to benefit from transparency firms must be candid and share all of their information on the blockchain. What happens if an actor is less than honest? Hence, a core research question motivating these structural drivers of malicious risk is: *What are the exogenous, structural mechanisms engendering the development of malicious supply chain risk?*

4.3 Macro-Drivers: Network Exposure

Research examining a firm's network exposure as a driver of malicious risk should seek to understand how different network structures in which firms are embedded can change their exposure to malicious risks. For example, highly central firms or firms with a high degree of connectivity to various firms might experience more exposure to malicious behavior. In addition, the influence of opportunistic behavior on a network could exhibit transitive properties such that malicious risks can spread throughout a network. Take, for example, the increasing role of Internet of things (IoT) and the connectivity across many different systems in a typical supply chain. What if, for example, an autonomous trailer is hacked by a malicious actor? The truck interacts with the firm via the cloud, and now, the hacker has the ability to steal data, corrupt systems, and so on. Thus, with increased connectivity comes increased risk, particularly as it is related to the firm's network. Thus, a motivating research question at this level is: *What role does the structure of the network in which a firm is embedded have on its susceptibility to/from malicious supply chain risk?*

5 Conclusion

Human beings hedging against risk can be seen as far back as the ancient Egyptians stockpiling grain as a mitigation tool against poor harvests (Levinson and Levinson 1985). Furthermore, while tools, techniques, and methods for dealing with risk have evolved into advanced systems, much of the research advocating prescriptive methodologies for managing risk focuses predominantly on inadvertent risk. The core thesis of this chapter is to shift the thinking, to focus on *malicious* risks, or those that are intentionally caused in the supply chain.

The reason for this need to examine, theorize against, and prescribe mechanisms for dealing with such risks is simple: Malicious risk can circumvent traditional supply chain risk management approaches. Effectively, the reason why malicious risks can be so pervasive is that their causes are quite different. Thus, in this vein we suggest that there are three core areas which drive malicious supply chain risk: behavioral-, structural-, and network-related engendering mechanisms. Further, research in this area is quite nascent with little, if any, work explicitly focused on these causes. Thus, as we enter the brave new world of supply chain risk management in the twenty-first century, our thinking needs to evolve with it. Traditional (inadvertent) risks and disruptions, though ever present, are also compounded by those intentional threats to normal operating conditions. Supply chain management needs to adjust its thinking to also consider how to thwart and minimize such risks. Moving forward, we are wise to remember the advice of Warren Buffet, "Risk comes from not knowing what you're doing."

References

Agrawal, A., & Muthulingam, S. (2015). Does organizational forgetting affect vendor quality performance? An empirical investigation. *Manufacturing & Service Operations Management, 17*(3), 350–367.

Ambulkar, S., Blackhurst, J., & Grawe, S. (2015). Firm's resilience to supply chain disruptions: Scale development and empirical examination. *Journal of Operations Management, 33,* 111–122.

Arnold, U., Neubauer, J., & Schoenherr, T. (2012). Explicating factors for companies' inclination towards corruption in Operations and supply chain management: An exploratory study in Germany. *International Journal of Production Economics, 138*(1), 136–147.

Babich, V., & Tang, C. S. (2012). Managing opportunistic supplier product adulteration: Deferred payments, inspection, and combined mechanisms. *Manufacturing & Service Operations Management, 14*(2), 301–314.

Barrett, S. R., Speth, R. L., Eastham, S. D., Dedoussi, I. C., Ashok, A., Malina, R., et al. (2015). Impact of the Volkswagen emissions control defeat device on US public health. *Environmental Research Letters, 10*(11), 114005.

Bhide, C. S. (2012). A study of the importance of forensic accounting in the modern business world. *DYPIMS's International Journal of Management and Research, 1*(1), 12–17.

Bonin, F., Devaux, B., & Dupré, A. (2006). *Turtles of the World*. Baltimore: JHU Press.

Brown, B. (2013). *Findus beef lasagne contained up to 100% horsemeat*. BBC News: FSA says.

Cheng, J.-H., & Chen, M.-C. (2016). Influence of institutional and moral orientations on relational risk management in supply chains. *Journal of Purchasing and Supply Management, 22*(2), 110–119.

Chopra, S., & Sodhi, M. S. (2004). Managing risk to avoid supply-chain breakdown. *MIT Sloan Management Review, 46*(1), 53.

Christopher, M., & Lee, H. (2004). Mitigating supply chain risk through improved confidence. *International Journal of Physical Distribution & Logistics Management, 34*(5), 388–396.

Daimler. (2017). Tracking down the product pirates. *Brand Protection.* Retrieved from https://www.daimler.com/sustainability/product/claim/brand-protection.html.

Doney, P. M., & Cannon, J. P. (1997). An examination of the nature of trust in buyer-seller relationships. *The Journal of Marketing*, 35–51.

DuHadway, S., Carnovale, S., & Hazen, B. (2017). Understanding risk management for intentional supply chain disruptions: Risk detection, risk mitigation, and risk recovery. *Annals of Operations Research*, 1–20.

Dwyer, F. R., Schurr, P. H., & Oh, S. (1987). Developing buyer-seller relationships. *The Journal of Marketing*, 11–27.

Finch, P. (2004). Supply chain risk management. *Supply Chain Management: An International Journal, 9*(2), 183–196.

Fisk, M. C., Mehrotra, K., Katz, A., & Plungis, J. (2016). Volkswagen agrees to $15 billion diesel-cheating settlement. *Bloomberg*. Retrieved from https://www.bloomberg.com/news/articles/2016-06-28/volkswagen-to-pay-14-7-billion-to-settle-u-s-emissions-claims.

Ganesan, S., & Hess, R. (1997). Dimensions and levels of trust: Implications for commitment to a relationship. *Marketing Letters, 8*(4), 439–448.

Garvey, M. D., Carnovale, S., & Yeniyurt, S. (2015). An analytical framework for supply network risk propagation: A Bayesian network approach. *European Journal of Operational Research, 242*(2), 618–627.

Giunipero, L. C., & Aly Eltantawy, R. (2004). Securing the upstream supply chain: A risk management approach. *International Journal of Physical Distribution & Logistics Management, 34*(9), 698–713.

Huang, X., Gattiker, T. F., & Schwarz, J. L. (2008). Interpersonal trust formation during the supplier selection process: The role of the communication channel. *Journal of Supply Chain Management, 44*(3), 53–75.

Kleindorfer, P. R., & Saad, G. H. (2005). Managing disruption risks in supply chains. *Production and Operations Management, 14*(1), 53–68.

Lee, H. L., & Whang, S. (2005). Higher supply chain security with lower cost: Lessons from total quality management. *International Journal of Production Economics, 96*(3), 289–300.

Levinson, H. Z., & Levinson, A. R. (1985). Storage and insect species of stored grain and tombs in ancient Egypt. *Zeitschrift für Angewandte Entomologie, 100*(1–5), 321–339.

Lippman, S. A., & Rumelt, R. P. (1982). Uncertain imitability: An analysis of interfirm differences in efficiency under competition. *The Bell Journal of Economics*, 418–438.

Liu, Y., Shankar, V., & Yun, W. (2017). Crisis management strategies and the long-term effects of product recalls on firm value. *Journal of Marketing, 81*(5), 30–48.

Madichie, N. O., & Yamoah, F. A. (2017). Revisiting the European horsemeat scandal: The role of power asymmetry in the food supply chain crisis. *Thunderbird International Business Review, 59*(6), 663–675.

McGreevy, C., & Harrop, W. (2015). Intentional cargo disruption by nefarious means: Examining threats, systemic vulnerabilities and securitisation measures in complex global supply chains. *Journal of business continuity & emergency planning, 8*(4), 326–345.

Morgan, R. M., & Hunt, S. D. (1994). The commitment-trust theory of relationship marketing. *The Journal of Marketing*, 20–38.

Nugent, T., Upton, D., & Cimpoesu, M. (2016). Improving data transparency in clinical trials using blockchain smart contracts. *F1000Research, 5*.

Parajuli, A., Kuzgunkaya, O., & Vidyarthi, N. (2017). Responsive contingency planning of capacitated supply networks under disruption risks. *Transportation Research Part E: Logistics and Transportation Review, 102,* 13–37.

Pettit, T. J., Simpson, N. C., Hancock, P. G., Clark, H., Haydel, T., & Pierce, J. (2016). Exploring operational resilience in the context of military aviation: Finding the right mode at the right time. *Journal of Business and Behavior Sciences, 28*(2), 24.

Pil, F. K., & Cohen, S. K. (2006). Modularity: Implications for imitation, innovation, and sustained advantage. *Academy of Management Review, 31*(4), 995–1011.

Rubel, O. (2018). Profiting from product-harm crises in competitive markets. *European Journal of Operational Research, 265*(1), 219–227.

Sapuric, S., & Kokkinaki, A. (2014). Bitcoin Is Volatile! Isn't that Right? In *Paper presented at the International Conference on Business Information Systems*.

Shah, R., Ball, G. P. & Netessine, S. (2017). Plant operations and product recalls in the automotive industry: An empirical investigation. *Management Science, 63*(8).

Sheffi, Y. (2001). Supply chain management under the threat of international terrorism. *The International Journal of Logistics Management, 12*(2), 1–11.

Suh, T., & Houston, M. B. (2010). Distinguishing supplier reputation from trust in buyer–supplier relationships. *Industrial Marketing Management, 39*(5), 744–751.

Tomlin, B. (2006). On the value of mitigation and contingency strategies for managing supply chain disruption risks. *Management Science, 52*(5), 639–657.

Trudell, C., & Fisk, M. C. (2016). Honda audit finds Takata engineers manipulated air-bag test data. *Bloomberg*. Retrieved July 18, 2016, from https://www.bloomberg.com/news/articles/2016-07-18/honda-audit-finds-takata-engineers-manipulated-air-bag-test-data.

Trudell, C., Hagiwara, Y., & Jie, M. (2014). Air-bag maker in global crisis used unusual explosive. *Bloomberg*. Retrieved October 26, 2014, from http://www.bloomberg.com/news/articles/2014-10-27/air-bag-maker-in-global-crisis-used-unusual-explosive.

Villena, V. H., & Craighead, C. W. (2017). On the same page? how asymmetric buyer-supplier relationships affect opportunism and performance. *Production and Operations Management, 26*(3), 491–508.

Vollmer, S. (2015). Monitoring fraud risks in the supply chain. *Journal of Accountancy, 219*(4), 26.

Warner, K., Timme, W., Lowell, B., & Hirshfield, M. (2013). Oceana study reveals seafood fraud nationwide. *Oceana, 11,* 1–69.

Williamson, O. E. (1985). *The economic intstitutions of capitalism*. New York: Simon and Schuster.

Woo, C. (2008). Mattels recalls (2007): Communication implications for quality control, outsourcing and consumer relations. *Arthur. W. Page Society, 2008 Case Study Competition*.

Wowak, K. D., & Boone, C. A. (2015). So many recalls, so little research: a review of the literature and road map for future research. *Journal of Supply Chain Management, 51*(4), 54–72.

Chapter 14
A Behavioural View of Supply Chain Risk Management

Mehrnoush Sarafan, Brian Squire and Emma Brandon-Jones

1 Behavioural Supply Chain Management

At its core, behavioural supply chain management studies the effect of human behaviour on supply chain operations and process performance, influenced by "cognitive biases, social preferences, and cultural norms" (Loch and Wu 2007, p. 15). Traditionally, operations and supply chain literature has examined various phenomenon from the lens of a rational decision-maker (Bendoly et al. 2006; Gino and Pisano 2008). This involves several implicit assumptions about the nature of human behaviour in the system; that is, people are (1) not the main phenomenon under study, (2) deterministic in their behaviour (e.g. they do not make mistakes; they are never influenced by their environment, beliefs and values), (3) independent and not affected by each other, (4) unchanging in their abilities and behaviours and (5) emotionless (Boudreau et al. 2003). There is evidence that individuals often violate these assumptions in a systematic manner, especially under situations of uncertainty (Kahneman and Tversky 1982). Simon (1979) argues that limitations in humans' memory, information gathering and computing ability constrain individuals to evaluate all possible alternatives under conditions of uncertainty and make fully rational decisions. Hence, the main purpose of behavioural research is to address the gap between the prediction of supply chain management theories and actual practices by accounting for the characteristics of human agents (e.g. beliefs,

M. Sarafan · B. Squire (✉)
HPC Supply Chain Innovation Lab, School of Management, University of Bath, Bath, UK
e-mail: B.C.Squire@bath.ac.uk

M. Sarafan
e-mail: M.Sarafan@bath.ac.uk

E. Brandon-Jones
School of Management, University of Bath, Bath, UK
e-mail: E.Brandon-Jones@bath.ac.uk

G. A. Zsidisin and M. Henke (eds.), *Revisiting Supply Chain Risk*, Springer Series in Supply Chain Management 7, https://doi.org/10.1007/978-3-030-03813-7_14

personalities, attitudes) and governance-influencing properties of supply chain systems (e.g. power-dependence, trust, relationship forms) (Gino and Pisano 2008; Tangpong et al. 2014). The research in this area has extensively leveraged the behavioural operations management (BeOM) and more broadly sociological and psychological perspectives in examining supply chain management phenomenon that might have been regarded as anomalies if seen from the lens of the traditional literature (Bendoly et al. 2009; Loch and Wu 2007; Tangpong et al. 2014).

Recent research in this area has explained the underlying mechanisms that shape managerial behaviour in newsvendor problems (e.g. Schweitzer and Cachon 2000; Véricourt et al. 2013), make-or-buy decisions (e.g. Mantel et al. 2006), supplier selection (e.g. Kull et al. 2014; Riedl et al. 2013), the bullwhip effect (e.g. Bolton and Katok 2008; Croson et al. 2014) and buyer–supplier relationships (e.g. Eckerd et al. 2016; Liu et al. 2012). For instance, in explaining behavioural sources of the bullwhip effect, Sterman and Dogan (2015) find that scarcity, especially when there is uncertainty about final demand, may cause anxiety, fear or panic, leading individuals to place much larger orders than they need when it is not rational to do so. In a similar vein, some studies have demonstrated the impact of cultural differences (Carter et al. 2010), risk perception and managerial illusions of control (Kull et al. 2014) on the outcome of supplier selection decisions. In general, recent behavioural research has contributed to the traditional literature by covering not only the properties of supply chain systems—e.g. structure, strategy, design—but also the characteristics of human agents—e.g. biases, personalities, preferences—who operate in such systems (Tangpong et al. 2014). This has, in turn, led to a better understanding of the underlying mechanisms of supply chain performance, as well as exploring intervention and institutional strategies such as training programmes and decision support systems that can reduce the effect of human biases (Bendoly et al. 2006; Gino and Pisano 2008; Loch and Wu 2007).

2 Supply Chain Risk Management: Limitations and Opportunities for Research

Supply chain risk management is essentially a decision-making process whereby managers evaluate the sources of supply chain risk and make decisions on whether to accept an assessed risk or implement strategies to reduce the probability and/or potential consequences of its occurrence (Manuj and Mentzer 2008; Norrman and Jansson 2004). Over the years, the literature has offered various risk management strategies, such as multiple sourcing (Hendricks et al. 2009), risk sharing (Nishat et al. 2006) and flexible transportation (Tang 2006), that may reduce the probability and/or firm's exposure to supply chain disruptions. These mitigation approaches have significant value in practice, including improved supply chain resilience, yielding higher supply base reliability (Tang 2006), lower system costs (Aqlan and Lam 2015), higher service levels (Wu et al. 2007) and shorter time to recovery (Sheffi and Rice 2005). However, a successful application of such strategies depends on the competence of supply chain managers and their ability to make crucial decisions when facing risk (Ambulkar et al. 2016).

To assist managers in such decision-making tasks, supply chain practitioners and scholars have developed risk management tools and frameworks (Kleindorfer and Saad 2005; Ritchie and Brindley 2007). The majority of these frameworks have made explicit and implicit assumptions on the nature of risk assessment and individuals' decision rules (Bendoly et al. 2006; Gino and Pisano 2008; Loch and Wu 2007). The accuracy of these assumptions has been questioned by behavioural research in analogous fields such as finance and recently by the supply chain risk literature. Our aim in the next two sections is to challenge these assumptions from a behavioural point of view and propose some avenues for future research.

2.1 Assumption 1: Objective Assessment of Risk

Risk assessment most commonly refers to an objective process of estimating the likelihood and potential consequences of a risky event, assigning significance to the impact and assessing the overall risk (Yates and Stone 1992). In the presence of historical data on the source and frequency of risks, this may be straightforward and can be done using quantitative techniques and statistical analysis. However, due to the global, dynamic and interdependent nature of the supply chain environment (Ellis et al. 2011), uncertainty is present in almost every risk management process and makes objective quantification of risk virtually impossible (Tazelaar and Snijders 2013; Vilko et al. 2014). Managers may face substantive uncertainty (Dosi and Egidi 1991) in the evaluation of supply chain risks because there is a lack of information about (a) the nature of an event, (b) the cause–effect relationships of an event (i.e. the lack of information about the location, severity and timing of an event) or (c) the value of available mitigation strategies (Milliken 1987). In addition, even when all necessary information is available, procedural uncertainty may limit their ability to process all of this information and pursue decision objectives (Dosi and Egidi 1991). To deal with such uncertainties, they instead rely on a range of socio-psychological processes and decision heuristics to form a subjective perception of risk (Sitkin and Pablo 1992), which will be subsequently used as the basis of their decision-making (Ellis et al. 2010; Ellis et al. 2011).

2.1.1 Subjective Risk Perception

Sitkin and Pablo (1992, p. 12) define risk perception as "a decision maker's assessment of the risk inherent in a situation". It guides individuals' evaluation and decisions about risk by influencing the information they attend to and/or utilise as the basis of their judgement (Sitkin and Pablo 1992). Risk perception is a *psychological factor* that is based on a variety of sources of information (Gierlach et al. 2010), but is mostly shaped by people's past experiences (Kull et al. 2014), beliefs (Douglas and Wildavsky 1983) and cultural factors (Dake 1992; Hsee and Weber 1999). These affect perceptions either through biasing the perception of overall risks (Douglas and Wildavsky 1983; Kahan et al. 2007) or individual components of risk—i.e. probability and consequences of outcome (Croson and Gneezy 2009; Gustafson 1998; Weber and Hsee 1998). For instance, Hsee and Weber (1999) find that cross-cultural differences systematically affect the level of perceived risk in different domains. For example, Chinese people perceive lower levels of financial risk compared to their American counterparts since they believe that their cultural group would financially support them if the risk led to catastrophic outcomes. Similarly, behavioural factors can affect the individual components of risk perception (Jia et al. 2015). For instance, technical experts might present a very accurate estimation of consequences of a risky event, but they still underestimate the probability of it happening (Slovic 1993). The effect of such behavioural factors on subjective perceptions of risk is mediated through two generic processes: (1) decision-makers' use of intuition and (2) sense-making. The following two sections will discuss these in more details.

2.1.2 Intuition

To deal with the complexity of supply chain problems and the limitations of their computational resources, managers often use their intuition, or what is commonly referred to as gut feeling (Stanczyk et al. 2015). Intuitive judgement is a *psychological evaluation process* based on people's non-conscious use of heuristics or cognitive schema (Dane and Pratt 2007; Fiske and Taylor 1991). Heuristics are simplifying mental strategies (i.e. shortcuts) that are utilised for quick and efficient processing of external information (Mishra 2014; Tversky and Kahneman 1973), while schema is defined as a complex structure of individual's beliefs, values and experiences stored in their social memory and representing knowledge about a particular concept (i.e. expectations about people, objects or social groups) (Fiske and Taylor 1991). At its core, schema function as a filter, guiding decision-makers to attend to what is important and help them to fill in gaps when information is missing or ambiguous (Gibson et al. 2009). Although intuition has been proved useful in solving a variety of complex problems (Dane and Pratt 2007; Issack 1978), it could also lead to systematic biases in decision-making (Carter et al. 2007; Kaufmann et al. 2014).

Research has identified a range of biases affecting individuals' judgement and decision-making in different contexts (Mishra 2014; Simon et al. 2000). A full review is beyond the scope of this chapter, but see Hogarth (1981), Carter et al. (2007) and Gino and Pisano (2008) for a list of frequently applied biases within the operations management context. To take one example, people are shown to often underestimate the possibility of downside risk and overestimate the chance of positive outcomes happening to them (Weinstein and Klein 1996). The phenomenon is referred to as unrealistic optimism or optimistic bias and could explain deviations from objective evaluations of risk based on people's belief that they are less likely than others to experience the negative consequences of risk (Breakwell 2014).

Furthermore, empirical evidence has provided insights into individual and cultural variations to the susceptibility of biases (e.g. Busenitz and Barney 1997; Stanovich and West 1998). For instance, Chui et al. (2010) find that in individualist cultures, where individual achievement and personal control are valued, people often fail to acknowledge the limitations of their knowledge and underestimate their likelihood of experiencing negative events (Helweg-Larsen and Shepperd 2001; Van den Steen 2004). Subsequently, they may perceive lower levels of risk compared to collectivist cultures when facing a similar situation (Rieger et al. 2015).

2.1.3 Sense-Making

Sense-making refers to a *socio-psychological process* that occurs when individuals face *discrepant cues* in their environment, and involves the *retrospective* development of a plausible mental model of the situation that facilitates information processing and decision-making (Maitlis and Sonenshein 2010; Olcott and Oliver 2014). It is particularly useful in resolving equivocality within a disruptive environment and shaping responses during and after an unexpected event (Ellis et al. 2011). Research in this area falls into two categories. The first group constitutes studies that focus on sense-making *during* a crisis as the event unfolds (e.g. Kayes 2004; Weick 1988; Wicks 2001). A well-known example is Weick's (1988) seminal study on Bhopal Accident that explains how an individual "confronts a puzzling assortment of dials, lights and sounds and discovers, through action, what the problem is, but in doing so, shapes the problem itself" (p. 306). The author argues that when facing an ambiguous environment, people often take actions (i.e. enact) to transform a complex situation into a simpler one. Subsequently, through interpretation and perception of their action (i.e. selection), they identify what the problem may have been, and whether their action was relevant and should be consolidated in the long term (i.e. retention). Within the supply chain risk literature, Ellis et al. (2011) draw from this perspective to develop a conceptual model that describes the underlying socio-psychological mechanisms of managerial decision-making in the face of supply chain disruption risks. The authors suggest that, facing a disruption, managers adopt a particular mitigation strategy (e.g. logistic integration, supplier development) that resolves equivocality in the situation. The efficacy of such a strategy in the long term is assessed by subjective perceptions of the magnitude and significance of losses following the action.

On the other hand, the second stream of sense-making studies is concerned with making sense of an event *after* it has occurred, i.e. how people interpret "what was the problem", "why did it happen" and "who was responsible" (Maitlis and Sonenshein 2010). For example, Olcott and Oliver (2014) use this view to study the development of organisational recovery capabilities and responses to the 2011 Japanese earthquake. In a similar vein, Coombs and Holladay (2002) focus on the public's attribution of responsibility following an organisational crisis (e.g. product recall, human breakdown accident) and the adoption of a firm's adoption of a response strategy to protect its reputation. A dominant theory used by these scholars is attribution theory, which examines the impact of attribution on people's emotion, expectation and future actions (Weiner 1985). For instance, recent studies have used the theory to understand the underlying factors that guide buyers' switching behaviour in the face of a psychological contract breach (Mir et al. 2017) and consumers' emotional responses to a firm's unsustainable behaviour (Hartmann and Moeller 2014).

Furthermore, a review of studies across both streams shows the importance of individual, organisational and situational factors in sense-making processes. For instance, drawing from enactment theory, Ellis et al. (2011) suggest that decentralisation and team diversity could reduce the level of equivocality in supply chain disruption situations, which in turn influence the sequence of activities in the sense-making process. Some scholars have also found that cultural backgrounds could affect the way in which people make sense of an event and attribute causes (Anagondahalli and Turner 2012; Martinko et al. 2007). For instance, Menon et al. (1999) show that individuals from collectivist cultures are more likely to attribute causes to contextual factors, while their counterparts from individualist cultures tend to focus on the individual actor.

2.1.4 Research Opportunities

The advance of behavioural research in supply chain management provides evidence on the importance of managerial perceptions of risk in decision-making (Tazelaar and Snijders 2013; Zsidisin 2003; Zsidisin and Wagner 2010). Ellis et al. (2010) draw from transaction cost economics (TCE) and resource dependence theory (RDT) to identify product- and market-related factors, such as product customisation and market thinness, that shape managers' overall perception of risk and in turn determine their choice of searching for an alternative supplier to manage risk. In a similar vein, Kull et al. (2014) show the effect of risk perception on the supplier selection process. Using a behavioural scenario-based experiment, the authors show that sourcing an important or difficult product category leads to higher levels of perceived risk, which subsequently increases preference for a supplier with more certain performance outcomes, even when that choice has a lower expected pay-off. Although these studies have started to explore behavioural factors that influence risk perception and risk-related decision-making, the literature is still in its infancy.

To improve the effectiveness of risk management practices, an explicit acknowledgement of behavioural factors and their impact on decision-making and perceptions of risk is crucial (Carter et al. 2007; Gino and Pisano 2008). Future studies could start to explore individual and cultural differences in cognitive biases and their consequences on managerial perceptions of risk in various contexts. In addition, researchers may use a range of quantitative and qualitative methods to empirically test the effect of behavioural factors on managerial sense-making during and after a disruptive event (Ellis et al. 2011). Identifying these factors and their impact on risk-related decision-making could help inform the design and development of incentive systems and situational interventions to improve decision consistency and minimise biases in managing risk (Sitkin and Pablo 1992). Potential research could seek to answer:

- How do individual differences (e.g. age, gender, experience) bias managerial perceptions of risk?
- How does culture affect managerial perceptions and management of supply chain risk?
- What are individual and contextual differences in managerial sense-making during a supply chain disruption and what are the consequences of this for the development of mitigation strategies in the long term?
- How do organisational factors (e.g. control systems, incentives, structures and systems) affect the managerial sense-making process?
- What shapes managerial sense-making (e.g. attribution of causes and responsibility) in the aftermath of a supply chain disruption? How does this influence firms' recovery responses?

2.2 Assumption 2: Rational Decision Rules

Traditionally, the literature has assumed that an individual's goals when confronted with a risk-based decision follow standard economic rules, such as cost minimisation or profit maximisation (Bendoly et al. 2006). Within the supply chain risk literature, a common objective is to optimise risk by balancing the overall costs of mitigation strategies with the potential financial consequences of a possible disruption (e.g. costs of switching a supplier with the financial losses of a supplier disruption) (Chopra and Sodhi 2004, 2014). On the other hand, there is evidence that supply chain managers may not always pursue optimisation in making such mitigation decisions (Carter et al. 2007). For example, a buyer may overly weight disruption costs because they believe that the supplier has violated the reciprocity of the relationship, or they may perceive lower switching costs since they have a lower propensity to tolerate risks involved in a status quo situation. The literature has suggested a range of individual and social preferences that may influence operational and relational decisions, such as newsvendor problems and contract design (e.g. Katok and Pavlov 2013; Loch and Wu 2007; Urda and Loch 2013). Here, we will focus on those that could potentially influence the overall goal of risk management models—i.e. risk optimisation.

2.2.1 Risk Propensity

Risk propensity is an individual characteristic that affects decision-making in the face of risk (Sitkin and Pablo 1992). People may be risk-averse with a strong tendency to avoid risks or risk-seeking enjoying the challenges involved in risky situations (Kocabasoglu et al. 2007). In general, there are two main conceptualisations of risk propensity in the literature. One stream views it as a general personality trait that is consistent in different contexts and stable across various situations (Bromiley and Curley 1992). These scholars use a range of personality features, such as sensation seeking (Zuckerman 1979, Horvath and Zuckerman 1993), impulsiveness (Eysenck and Eysenck 1978), openness (McCrae and Costa 1997) or decision-making style (Franken 1988) to demonstrate the individual differences in risk behaviour. Apart from psychological traits, demographic and socio-economic characteristics, such as gender (Byrnes et al. 1999), age (Cauffman et al. 2010) and job function (Steward and Roth 2001), have been also shown to correlate with individuals' preferences towards risk.

On the other hand, the second stream theorises risk propensity as an individual's characteristic which varies in different situations and decision domains (Weber et al. 2002). In other words, individuals cannot be categorised as general risk seekers or averters; instead, they are likely to be consistently seeking risk in certain areas of their life (e.g. business) and reluctant to take risk in others (e.g. personal) (Maccrimmon and Wehrung 2014; Nicholson et al. 2005). Within this stream, some scholars (e.g. Sitkin and Pablo 1992) also argue that risk propensity is persistent at a single point in time, but can evolve as people gain more experience. These authors suggest that dispositional risk preferences, individuals' routine ways of handling risk, and prior failure or success outcomes could all influence people's risk propensity at any point in time. Regardless of the theoretical differences, the evidence presented here highlights individual and/or situational variations in attitude towards risk, which in turn could have consequences for managerial decision-making in the face of supply chain risk.

2.2.2 Social Preferences

Traditionally, people are assumed to be *self-interested* and *rational* agents who only consider their own pay-off when making economic decisions (Loch and Wu 2007). Accordingly, research has utilised various forms of economic incentives to promote cooperative behaviour between buyer and supplier agents (for an overview, see Cachon 2003). However, recent advancements in behavioural research suggest that in a social setting, such as the supply chain environment, individuals pursue social preferences and care about others' pay-off as much as their own economic benefits (Ho et al. 2014; Urda and Loch 2013). In particular, people have emotionally based social goals that guide their behaviour in social interactions to pursue *group identity*, *reciprocity* and *status* (Loch and Wu 2008). These reflect an individual's interests in their partners' benefits as well as their own, concerns for responding to a history of successful/unsuccessful relationships, and competitive behaviour to gain or deny higher status in a social group. For example, Loch and Wu (2008) find that the experience of a "friendly" relationship in a buyer–supplier relationship can motivate mutually beneficial actions, while status-seeking can impact partners' attitude to act more competitively in a pricing game. The results from this and similar studies highlight that standard economic incentives are not the only factors that influence people's behaviour. Instead, salient social components can operate as substitutes or partial complements to formal incentive systems and serve as motivational factors in decision-making processes.

Scholars have previously demonstrated the impact of social preferences on various supply chain phenomenon (e.g. Cui et al. 2007; Ho et al. 2014). In particular, fairness is shown to be closely related to preferences for status and reciprocity, and influences people's behaviour in buyer–supplier interactions (Cui et al. 2007; Fehr and Schmidt 1999). Within such relationships, partners design and negotiate contracts that rely on the fundamentals of reciprocity and fairness—desire to be treated and treat others fairly (Katok and Pavlov 2013). They share information and resources with each other even when it is counter-productive to do so (Katok and Pavlov 2013). For example, Liu et al. (2012) find that a positive perception of fairness in a buyer–supplier relationship could result in higher knowledge sharing, joint investment in facilities and personnel, and continuous relationship commitment. Nevertheless, it is also not uncommon that a supply chain partner is punished for its unfair actions (Kumar et al. 1998). For instance, Wang et al. (2014) find empirical evidence highlighting the buyers' perception of injustice during a disruption resolution process could lead to trust damage and, subsequently, termination of the buyer–supplier relationship.

2.2.3 Research Opportunities

Empirical research has demonstrated the importance of top managers' risk propensity in shaping various operational decisions (Das and Teng 2001; Hung and Tangpong 2010). For example, risk-averse newsvendors are shown to have a lower tendency towards uncertain outcomes (i.e. variant pay-offs) and hence are likely to order less compared to their risk-neutral counterparts (Véricourt et al. 2013). On the other hand, risk-seeking managers are evidently more keen to choose a supplier with more uncertain performance outcomes in the hope of achieving higher pay-offs (Kull et al. 2014). Within supply chain literature, the majority of risk management frameworks have so far neglected individual and contextual differences in managerial risk propensity. This provides a great opportunity for future behavioural works to seek answers for the following question:

- How and when does top managers' risk propensity affect responses to an impending disruption?

Furthermore, supply chain disruptions are interorganisational phenomenon that occurs within a relationship-specific context (Bode et al. 2011). Hence, social preferences most likely play an important role in shaping both buyers' and suppliers' behaviour towards risk. Previous research has already highlighted the importance of trust (Bode et al. 2011) and justice (Wang et al. 2014) in managing the consequences of such events. Future work in this area could start exploring:

- How could social preferences for status-seeking affect the development of collaborative risk management strategies?
- How do social preferences for status-seeking shape buyers' and suppliers' responses to a supply chain disruption event?
- How do social preferences for group identity contribute to the development of collaborative risk management strategies?
- How does the perception of fairness influence firms' responses to a supply chain disruption?

3 Conclusion

We draw from advances in behavioural research in operations and supply chain management to highlight the importance of incorporating a behavioural view in supply chain risk management studies. The majority of existing risk management models and frameworks have so far ignored the role of individual agents in evaluating supply chain risks and making mitigation decisions. Managers are assumed to have access to all necessary information in their environment, show consistent preferences, and use all time and computational resources to calculate objective risk and choose an optimal mitigation strategy. However, we observe many anomalies in practice. In this chapter, we discuss some of the most important behavioural factors that could systematically influence decision-makers' risk assessment and potentially influence their decisions in the face of risk. We hope that our review encourages more scholars to pursue a behavioural perspective in developing risk management models and provides opportunities for future research to examine individual, situational and contextual variations in planning and/or responding to supply chain disruptions.

References

Ambulkar, S., Blackhurst, J. V., & Cantor, D. E. (2016). Supply chain risk mitigation competency: an individual-level knowledge-based perspective. *International Journal of Production Research, 54*(5), 1398–1411. https://doi.org/10.1080/00207543.2015.1070972.

Anagondahalli, D., & Turner, M. M. (2012). Predicting psychological ripple effects: The role of cultural identity, in-group/out-group identification, and attributions of blame in crisis communication. *Risk Analysis, 32*(4), 695–712. https://doi.org/10.1111/j.1539-6924.2011.01727.x.

Aqlan, F., & Lam, S. S. (2015). Supply chain risk modelling and mitigation. *International Journal of Production Research, 53*(18), 5640–5656. https://doi.org/10.1080/00207543.2015.1047975.

Bendoly, E., Croson, R., & Schu, K. (2009). Bodies of knowledge for research in behavioral operations. *Production and Operations Management, 19*(4), 434–452. https://doi.org/10.3401/poms.1080.01108.

Bendoly, E., Donohue, K., & Schultz, K. L. (2006). Behavior in operations management: Assessing recent findings and revisiting old assumptions. *Journal of Operations Management, 24*(6), 737–752. https://doi.org/10.1016/j.jom.2005.10.001.

Bode, C., Wagner, S. M., Petersen, K. J., & Ellram, L. M. (2011). Understanding responses to supply chain disruptions: Insights from information processing and resource dependence perspectives. *Academy of Management Journal, 54*(4), 833–856. https://doi.org/10.5465/AMJ.2011.64870145.

Bolton, G. E., & Katok, E. (2008). Learning by doing in the newsvendor problem: A laboratory investigation of the role of experience and feedback. *Manufacturing & Service Operations Management, 10*(3), 519–538. https://doi.org/10.1287/msom.1060.0190.

Boudreau, J., Hopp, W., McClain, J. O., & Thomas, L. J. (2003). Commissioned paper: On the interface between operations and human resources management. *Manufacturing & Service Operations Management, 5*(3), 179–202. https://doi.org/10.1287/msom.5.3.179.16032.

Breakwell, D. G. M. (2014). *The psychology of risk*. Cambridge, UK: Cambridge University Press. https://doi.org/10.1017/CBO9781139061933.

Bromiley, P., & Curley, S. P. (1992). Individual differences in risk taking. In J. F. Yades (Ed.), *Risk-taking behavior* (pp. 87–132). Oxford, England: Wiley.

Busenitz, L. W., & Barney, J. B. (1997). Differences between entrepreneurs and managers in large organizations: Biases and heuristics in strategic decision-making. *Journal of Business Venturing, 12*(1), 9–30. https://doi.org/10.1016/S0883-9026(96)00003-1.

Byrnes, J., Miller, D., & Schafer, W. (1999). Gender differences in risk taking. *Psychological Bulletin, 125*(3), 367–383. https://doi.org/10.1037/0033-2909.125.3.367.

Cachon, G. P. (2003). Supply chain coordination with contracts. *Handbooks in Operations Research and Management Science, 11,* 227–339. https://doi.org/10.1016/S0927-0507(03)11006-7.

Carter, C. R., Kaufmann, L., & Michel, A. (2007). Behavioral supply management: a taxonomy of judgment and decision-making biases. *International Journal of Physical Distribution & Logistics Management, 37*(8), 631–669. https://doi.org/10.1108/09600030710825694.

Carter, J. R., Maltz, A., Maltz, E., Goh, M., & Yan, T. (2010). Impact of culture on supplier selection decision making. *The International Journal of Logistics Management, 21*(3), 353–374. https://doi.org/10.1108/09574091011089790.

Cauffman, E., Shulman, E. P., Steinberg, L., Claus, E., Banich, M. T., Graham, S., et al. (2010). Age differences in affective decision making as indexed by performance on the Iowa Gambling Task. *Developmental Psychology, 46*(1), 193–207. https://doi.org/10.1037/a0016128.

Chopra, S., & Sodhi, M. S. (2004). Managing risk to avoid supply-chain breakdown. *MIT Sloan Management Review, 46*(1), 53–61. https://doi.org/10.1108/IJOPM-10-2012-0449.

Chopra, S., & Sodhi, M. S. (2014). Reducing the risk of supply chain disruptions. *MIT Sloan Management Review, 55*(3), 73–80. https://doi.org/10.1017/CBO9781107415324.004.

Chui, A. C. W., Titman, S., & Wei, K. C. J. (2010). Individualism and momentum around the world. *The Journal of Finance, 65*(1), 361–392. https://doi.org/10.1111/j.1540-6261.2009.01532.x.

Coombs, W. T., & Holladay, S. J. (2002). Helping crisis managers protect reputational assets: initial tests of the situational crisis communication theory. *Management Communication Quarterly, 16*(2), 165–186. https://doi.org/10.1177/089331802237233.

Croson, R., Donohue, K., Katok, E., & Sterman, J. (2014). Order stability in supply chains: Coordination risk and the role of coordination stock. *Production and Operations Management, 23*(2), 176–196. https://doi.org/10.1111/j.1937-5956.2012.01422.x.

Croson, R., & Gneezy, U. (2009). Gender differences in preferences. *Journal of Economic Literature, 47*(2), 448–474. https://doi.org/10.1257/jel.47.2.448.

Cui, T. H., Raju, J. S., & Zhang, Z. J. (2007). Fairness and channel coordination. *Management Science, 53*(8), 1303–1314. https://doi.org/10.1287/mnsc.1060.0697.

Dake, K. (1992). Myths of nature: Culture and the social construction of risk. *Journal of Social Issues, 48*(4), 21–37. https://doi.org/10.1111/j.1540-4560.1992.tb01943.x.

Dane, E., & Pratt, M. G. (2007). Exploring intuition and its role in managerial decision making. *Academy of Management Review, 32*(1), 33–54. https://doi.org/10.5465/AMR.2007.23463682.

Das, T. K., & Teng, B.-S. (2001). Strategic risk behaviour and Its temporalities: Between risk propensity and decision context. *Journal of Management Studies, 38*(4), 515–534. https://doi.org/10.1111/1467-6486.00247.

Dosi, G., & Egidi, M. (1991). Substantive and procedural uncertainty—An exploration of economic behaviours in changing environments. *Journal of Evolutionary Economics, 1*(2), 145–168. https://doi.org/10.1007/BF01224917.

Douglas, M., & Wildavsky, A. (1983). *Risk and culture*. Berkeley and Los Angeles, California: University of California Press. https://doi.org/10.1093/oxfordhb/9780195396430.013.0028.

Eckerd, S., Boyer, K. K., Eckerd, A., & Hill, J. A. (2016). Supply chain psychological contract breach: An experimental study across national cultures. *Journal of Supply Chain Management, 52*(3), 68–82. https://doi.org/10.1111/jscm.12101.

Ellis, S. C., Henry, R. M., & Shockley, J. (2010). Buyer perceptions of supply disruption risk: A behavioral view and empirical assessment. *Journal of Operations Management, 28*(1), 34–46. https://doi.org/10.1016/j.jom.2009.07.002.

Ellis, S. C., Shockley, J., & Henry, R. M. (2011). Making sense of supply disruption risk research: A conceptual framework grounded in enactment theory. *Journal of Supply Chain Management, 47*(2), 65–96. https://doi.org/10.1111/j.1745-493X.2011.03217.x.

Eysenck, S. B. G., & Eysenck, H. J. (1978). Impulsiveness and venturesomeness: Their position in a dimensional system of personality description. *Psychological Reports*, *43*(3 suppl), 1247–1255. https://doi.org/10.2466/pr0.1978.43.3f.1247.

Fehr, E., & Schmidt, K. M. (1999). A theory of fairness, competition, and cooperation. *The Quarterly Journal of Economics, 114*(3), 817–868. https://doi.org/10.1162/003355399556151.

Fiske, S. T., & Taylor, S. E. (1991). *Social cognition: From brains to culture* (1st ed.). New York: McGraw-Hill.

Franken, R. E. (1988). Sensation seeking, decision making styles, and preference for individual responsibility. *Personality and Individual Differences, 9*(1), 139–146. https://doi.org/10.1016/0191-8869(88)90039-6.

Gibson, C. B., Maznevski, M. L., & Kirkman, B. L. (2009). When does culture matter. In R. S. Bhagat & R. M. Steers (Eds.), *Cambridge handbook of culture, organizations, and work* (pp. 46–68). Cambridge, UK: Cambridge University Press.

Gierlach, E., Belsher, B. E., & Beutler, L. E. (2010). Cross-cultural differences in risk perceptions of disasters. *Risk Analysis, 30*(10), 1539–1549. https://doi.org/10.1111/j.1539-6924.2010.01451.x.

Gino, F., & Pisano, G. (2008). Toward a theory of behavioral operations. *Manufacturing & Service Operations Management, 10*(4), 676–691. https://doi.org/10.1287/msom.1070.0205.

Gustafson, P. E. (1998). Gender differences in risk perception: Theoretical and methodological perspectives. *Risk Analysis, 18*(6), 805–811. https://doi.org/10.1023/B:RIAN.0000005926.03250.c0.

Hartmann, J., & Moeller, S. (2014). Chain liability in multitier supply chains? Responsibility attributions for unsustainable supplier behavior. *Journal of Operations Management, 32*(5), 281–294. https://doi.org/10.1016/j.jom.2014.01.005.

Helweg-Larsen, M., & Shepperd, J. A. (2001). Do moderators of the optimistic bias affect personal or target risk estimates? A review of the literature. *Personality and Social Psychology Review, 5*(1), 74–95. https://doi.org/10.1207/S15327957PSPR0501_5.

Hendricks, K. B., Singhal, V. R., & Zhang, R. (2009). The effect of operational slack, diversification, and vertical relatedness on the stock market reaction to supply chain disruptions. *Journal of Operations Management, 27*(3), 233–246. https://doi.org/10.1016/j.jom.2008.09.001.

Ho, T. H., Su, X., & Wu, Y. (2014). Distributional and peer-induced fairness in supply chain contract design. *Production and Operations Management, 23*(2), 161–175. https://doi.org/10.1111/poms.12064.

Hogarth, R. M. (1981). Beyond discrete biases: Functional and dysfunctional aspects of judgmental heuristics. *Psychological Bulletin, 90*(2), 197–217. https://doi.org/10.1037/0033-2909.90.2.197.

Horvath, P., & Zuckerman, M. (1993). Sensation seeking, risk appraisal, and risky behaviour. *Personality and individual difference*, *14*(1), 47–52.

Hsee, C. K., & Weber, E. U. (1999). Cross-cultural differences in risk preference and lay predictions. *Journal of Behavioral Decision Making, 12*(2), 165–179. https://doi.org/10.1002/(SICI)1099-0771(199906)12.

Hung, K. T., & Tangpong, C. (2010). General risk propensity in multifaceted business decisions: Scale development. *Journal of Managerial Issues*, *22*(1), 88–106. Retrieved from http://www.jstor.org/stable/25822517.

Issack, T. S. (1978). Intuition: An ignored dimension of management. *Academy of Management Review, 3*(4), 917–922. https://doi.org/10.5465/AMR.1978.4289310.

Jia, J. S., Khan, U., & Litt, A. (2015). The effect of self-control on the construction of risk perceptions. *Management Science, 61*(9), 2259–2280. https://doi.org/10.1287/mnsc.2014.2098.

Kahan, D. M., Braman, D., Gastil, J., Slovic, P., & Mertz, C. K. (2007). Culture and identity-protective cognition: Explaining the white-male effect in risk perception. *Journal of Empirical Legal Studies, 4*(3), 465–505. https://doi.org/10.1111/j.1740-1461.2007.00097.x.

Kahneman, D., & Tversky, A. (1982). Variants of uncertainty. *Cognition, 11*(2), 143–157.

Katok, E., & Pavlov, V. (2013). Fairness in supply chain contracts: A laboratory study. *Journal of Operations Management, 31*(3), 129–137. https://doi.org/10.1016/j.jom.2013.01.001.

Kaufmann, L., Meschnig, G., & Reimann, F. (2014). Rational and intuitive decision-making in sourcing teams: Effects on decision outcomes. *Journal of Purchasing and Supply Management, 20*(2), 104–112. https://doi.org/10.1016/j.pursup.2014.03.003.

Kayes, D. C. (2004). The 1996 Mount Everest climbing disaster: The breakdown of learning in teams. *Human Relations, 57*(10), 1263–1284. https://doi.org/10.1177/0018726704048355.

Kleindorfer, P. R., & Saad, G. H. (2005). Managing disruption risks in supply chains. *Production and Operations Management, 14*(1), 53–68. https://doi.org/10.1111/j.1937-5956.2005.tb00009.x.

Kocabasoglu, C., Prahinski, C., & Klassen, R. D. (2007). Linking forward and reverse supply chain investments: The role of business uncertainty. *Journal of Operations Management, 25*(6), 1141–1160. https://doi.org/10.1016/j.jom.2007.01.015.

Kull, T. J., Oke, A., & Dooley, K. J. (2014). Supplier selection behavior under uncertainty: Contextual and cognitive effects on risk perception and choice. *Decision Sciences, 45*(3), 467–505. https://doi.org/10.1111/deci.12078.

Kumar, N., Scheer, L. K., & Steenkamp, J. B. E. M. (1998). Interdependence, punitive capability, and the reciprocation of punitive actions in channel relationships. *Journal of Marketing Research, 35*(2), 225–235. https://doi.org/10.2307/3151850.

Liu, Y., Huang, Y., Luo, Y., & Zhao, Y. (2012). How does justice matter in achieving buyer—Supplier relationship performance? *Journal of Operations Management, 30*(5), 355–367. https://doi.org/10.1016/j.jom.2012.03.003.

Loch, C. H., & Wu, Y. (2007). Behavioral operations management. *Foundations and Trends in Technology, Information and Operations Management, 1*(3), 121–232. https://doi.org/10.1561/0200000009.

Loch, C. H., & Wu, Y. Z. (2008). Social preferences and supply chain performance: An experimental study. *Management Science, 54*(11), 1835–1849. https://doi.org/10.1287/mnsc.1080.0910.

Maccrimmon, K. R., & Wehrung, D. A. (2014). Characteristics of risk taking executives. *Management Science, 36*(4), 422–435. https://doi.org/10.1287/mnsc.36.4.422.

Maitlis, S., & Sonenshein, S. (2010). Sensemaking in crisis and change: Inspiration and insights from weick (1988). *Journal of Management Studies, 47*(3), 551–580. https://doi.org/10.1111/j.1467-6486.2010.00908.x.

Mantel, S. P., Tatikonda, M. V., & Liao, Y. (2006). A behavioral study of supply manager decision-making: Factors influencing make versus buy evaluation. *Journal of Operations Management, 24*(6), 822–838. https://doi.org/10.1016/j.jom.2005.09.007.

Manuj, I., & Mentzer, J. T. (2008). Global supply chain risk management strategies. *International Journal of Physical Distribution & Logistics Management, 38*(3), 192–223. https://doi.org/10.1108/09600030810866986.

Martinko, M. J., Harvey, P., & Douglas, S. C. (2007). The role, function, and contribution of attribution theory to leadership: A review. *The Leadership Quarterly, 18*(6), 561–585. https://doi.org/10.1016/j.leaqua.2007.09.004.

McCrae, R. R., & Costa, P. T. (1997). Conceptions and correlates of openness to experience. In R. Hogan, J. Johnson & S. Briggs (Eds.), *Handbook of personality psychology* (pp. 825–847). California: Academic Press. https://doi.org/10.1016/B978-012134645-4/50032-9.

Menon, T., Morris, M. W., Chiu, C. Y., & Hong, Y. Y. (1999). Culture and the construal of agency: Attribution to individual versus group dispositions. *Journal of Personality and Social Psychology, 76*(5), 701–717. https://doi.org/10.1037/0022-3514.76.5.701.

Milliken, F. J. (1987). Three types of perceived uncertainty about the environment: State, effect, and response uncertainty. *Academy of Management Review, 12*(1), 133–143. https://doi.org/10.5465/AMR.1987.4306502.

Mir, S., Aloysius, J. A., & Eckerd, S. (2017). Understanding supplier switching behavior: The role of psychological contracts in a competitive setting. *Journal of Supply Chain Management, 53*(3), 3–18. https://doi.org/10.1111/jscm.12115.

Mishra, S. (2014). Decision-making under risk: Integrating perspectives from biology, economics, and psychology. *Personality and Social Psychology Review : An Official Journal of* *the Society for Personality and Social Psychology, Inc*, *18*(3), 280–307. https://doi.org/10.1177/1088868314530517.

Nicholson, N., Soane, E., Fenton-O'Creevy, M., & Willman, P. (2005). Personality and domain-specific risk taking. *Journal of Risk Research, 8*(2), 157–176. https://doi.org/10.1080/1366987032000123856.

Nishat Faisal, M., Banwet, D. K., & Shankar, R. (2006). Supply chain risk mitigation: modeling the enablers. *Business Process Management Journal, 12*(4), 535–552. https://doi.org/10.1108/14637150610678113.

Norrman, A., & Jansson, U. (2004). Ericsson's proactive supply chain risk management approach after a serious sub-supplier accident. *International Journal of Physical Distribution & Logistics Management, 34*(5), 434–456. https://doi.org/10.1108/09600030410545463.

Olcott, G., & Oliver, N. (2014). Social capital, sensemaking, and recovery: Japanese companies and the 2011 earthquake. *California Management Review, 56*(2), 5–22. https://doi.org/10.1525/cmr.2014.56.2.5.

Riedl, D. F., Kaufmann, L., Zimmermann, C., & Perols, J. L. (2013). Reducing uncertainty in supplier selection decisions: Antecedents and outcomes of procedural rationality. *Journal of Operations Management, 31*(1–2), 24–36. https://doi.org/10.1016/j.jom.2012.10.003.

Rieger, M. O., Wang, M., & Hens, T. (2015). Risk preferences around the world. *Management Science, 61*(3), 637–648. https://doi.org/10.1287/mnsc.2013.1869.

Ritchie, B., & Brindley, C. (2007). Supply chain risk management and performance: A guiding framework for future development. *International Journal of Operations and Production Management, 27*(3), 303–322. https://doi.org/10.1108/01443570710725563.

Schweitzer, M. E., & Cachon, G. P. (2000). Decision bias in the newsvendor problem with a known demand distribution: Experimental evidence. *Management Science, 46*(3), 404–420. https://doi.org/10.1287/mnsc.46.3.404.12070.

Sheffi, Y., & Rice, J. B., Jr. (2005). A supply chain view of the resilient enterprise. *MIT Sloan Management Review, 47*(1), 41–48. https://doi.org/10.1007/978-0-387-79933-9.

Simon, H. (1979). Rational decision making in business organizations. *The American Economic Review, 69*(4), 493–513. Retrieved from http://www.jstor.org/stable/1808698.

Simon, M., Houghton, S. M., & Aquino, K. (2000). Cognitive biases, risk perception, and venture formation: How individuals decide to start companies. *Journal of Business Venturing, 15*(98), 113–134. https://doi.org/10.1016/S0883-9026(98)00003-2.

Sitkin, S. B., & Pablo, A. L. (1992). Reconceptualizing the determinants of risk behavior. *The Academy of Management Review, 17*(1), 9–38. https://doi.org/10.5465/AMR.1992.4279564.

Slovic, P. (1993). Perceived risk, trust, and democracy. *Risk Analysis, 13*(6), 675–682. https://doi.org/10.1111/j.1539-6924.1993.tb01329.x.

Stanczyk, A., Foerstl, K., Busse, C., & Blome, C. (2015). Global sourcing decision-making processes: Politics, intuition, and procedural rationality. *Journal of Business Logistics, 36*(2), 160–181. https://doi.org/10.1111/jbl.12090.

Stanovich, K. E., & West, R. F. (1998). Individual differences in rational thought. *Journal of Experimental Psychology: General, 127*(2), 161–188. https://doi.org/10.1037/0096-3445.127.2.161.

Sterman, J. D., & Dogan, G. (2015). "I'm not hoarding, I'm just stocking up before the hoarders get here": Behavioral causes of phantom ordering in supply chains. *Journal of Operations Management, 39–40,* 6–22. https://doi.org/10.1016/j.jom.2015.07.002.

Steward, W. H., & Roth, P. L. L. (2001). Risk propensity differences between entrepreneurs and managers: A meta-analytic review. *Journal of Applied Psychology, 86*(1), 145–153. https://doi.org/10.1037//0021-9010.86.1.145.

Tang, C. (2006). Robust strategies for mitigating supply chain disruptions. *International Journal of Logistics, 9*(1), 33–45. https://doi.org/10.1080/13675560500405584.

Tangpong, C., Hung, K. T., & Li, J. (2014). Agent-system co-development in supply chain research: Propositions and demonstrative findings. *Journal of Operations Management, 32*(4), 154–174. https://doi.org/10.1016/j.jom.2014.03.002.

Tazelaar, F., & Snijders, C. (2013). Operational risk assessments by supply chain professionals: Process and performance. *Journal of Operations Management, 31*(1–2), 37–51. https://doi.org/10.1016/j.jom.2012.11.004.

Tversky, A., & Kahneman, D. (1973). Availability: A heuristic for judging frequency and probability. *Cognitive Psychology, 5*(2), 207–232. https://doi.org/10.1016/0010-0285(73)90033-9.

Urda, J., & Loch, C. H. (2013). Social preferences and emotions as regulators of behavior in processes. *Journal of Operations Management, 31*(1–2), 6–23. https://doi.org/10.1016/j.jom.2012.11.007.

Van den Steen, E. (2004). Rational overoptimism (and other biases). *American Economic Review, 94*(4), 1141–1151. https://doi.org/10.1257/0002828042002697.

Véricourt, F. De, Jain, K., Bearden, J. N., & Filipowicz, A. (2013). Sex, risk and the newsvendor. *Journal of Operations Management, 31*(1–2), 86–92. https://doi.org/10.1016/j.jom.2012.11.001.

Vilko, J., Ritala, P., & Edelmann, J. (2014). On uncertainty in supply chain risk management. *International Journal of Logistics Management, 25*(1), 3–19. https://doi.org/10.1108/IJLM-10-2012-0126.

Wang, Q., Craighead, C. W., & Juan, J. (2014). Justice served: Mitigating damaged trust stemming from supply chain disruptions. *Journal of Operations Management, 32*(6), 374–386. https://doi.org/10.1016/j.jom.2014.07.001.

Weber, E. U., Blais, A. R., & Betz, N. E. (2002). A domain-specific risk-attitude scale: Measuring risk perceptions and risk behaviors. *Journal of Behavioral Decision Making, 15*(4), 263–290. https://doi.org/10.1002/bdm.414.

Weber, E. U., & Hsee, C. (1998). Cross-cultural differences in risk perception, but cross-cultural similarities in attitudes towards perceived risk. *Management Science*, *44*(9), 7205–7277.

Weick, K. E. (1988). Enacted sensemaking in crisis situations. *Journal of Management Studies, 25*(4), 305–317. https://doi.org/10.1111/j.1467-6486.1988.tb00039.x.

Weiner, B. (1985). An attributional theory of achievement motivation and emotion. *Psychological Review, 92*(4), 548–573. https://doi.org/10.1037/0033-295X.92.4.548.

Weinstein, N. D., & Klein, W. M. (1996). Unrealistic optimism: Present and future. *Journal of Social and Clinical Psychology, 15*(1), 1–8. https://doi.org/10.1521/jscp.1996.15.1.1.

Wicks, D. (2001). Institutionalized mindsets of invulnerability: Differentiated institutional fields and the antecedents of organizational crisis. *Organization Studies, 22*(4), 659–692. https://doi.org/10.1177/0170840601224005.

Wu, T., Blackhurst, J., & O'Grady, P. (2007). Methodology for supply chain disruption analysis. *International Journal of Production Research, 45*(7), 1665–1682. https://doi.org/10.1080/00207540500362138.

Yates, J. F., & Stone, E. R. (1992). Risk appraisal. In J. F. Yates (Ed.), *Wiley series in human performance and cognition. Risk-taking behavior* (pp. 49–85). Oxford, England: Wiley.

Zsidisin, G. A. (2003). Managerial perceptions of supply risk. *Journal of Supply Chain Management, 39*(November), 14–26. https://doi.org/10.1111/j.1745-493X.2003.tb00146.x.

Zsidisin, G. A., & Wagner, S. M. (2010). Do perceptions become reality? The moderating role of supply chain resiliency on disruption occurrence. *Journal of Business Logistics, 31*(2), 1–20. https://doi.org/10.1002/j.2158-1592.2010.tb00140.x.

Zuckerman, M. (1979). Sensation seeking and risk taking. In *Emotions in personality and psychopathology* (pp. 767–797). Springer, Boston, MA.

Part IV
Managing Risk in Sustainable and Innovative Supply Chains

Chapter 15
Resilience and Sustainability in Supply Chains

Holmes E. Miller and Kurt J. Engemann

1 Introduction

Supply chain resilience and supply chain sustainability are well-accepted and well-examined concepts. On the surface, as with low costs and high quality, they may appear to require either/or trade-offs, rather than be mutually supportive. For example, strategies to enhance supply chain resilience may involve many suppliers and relax guidelines regarding supplier behavior. Strategies to enhance supply chain sustainability may create constraints that some might argue detract from resilience. Yet first impressions often can be misleading. In this chapter, we will examine supply chain resilience and supply chain sustainability separately and then discuss how the concepts in many ways are mutually supportive rather than conflicting. This symbiosis not only is true today, but will increase as business practices, information technologies, and customer preferences evolve.

While each of the above concepts has been thoroughly examined when considered separately, less research and guidelines exist for practice regarding their intersection. This creates a potential gap, where advancements in research and practice for supply chain resilience and supply chain sustainability might proceed in parallel, but potentially may result in conflicting strategies and operational tactics. Examples might involve supply chain architectures that are resilient but which fail to effectively address sustainability criteria, such as working conditions or meeting environmental standards. Or, supply chain architectures that are sound regarding all sustainabil-

H. E. Miller (✉)
Department of Accounting, Business, Economics, and Finance, Muhlenberg College, Allentown, PA 18104, USA
e-mail: holmesmiller@muhlenberg.edu

K. J. Engemann
Center for Business Continuity and Risk Management, Iona College, New Rochelle, NY 10801, USA
e-mail: kengemann@iona.edu

G. A. Zsidisin and M. Henke (eds.), *Revisiting Supply Chain Risk*, Springer Series in Supply Chain Management 7, https://doi.org/10.1007/978-3-030-03813-7_15

ity criteria, but which are riddled with risks leaving the supply chain vulnerable to shocks to the system.

To address this gap, we develop a framework that mutually addresses possible scenarios and presents "sample possible behaviors" where supply chain resilience categories intersect with categories related to sustainability. Our goal is to develop a frame of reference to address potential conflicts and to create solutions, that not only are resilient and sustainable in the sense mentioned above, but also resilient and sustainable in being able to bounce back from shocks and operation over the long haul.

Before analyzing each concept, we will define terms more explicitly. A resilient supply chain is one supporting a company that can, as just noted, "bounce back from a large disruption—this includes, for instance, the speed with which it returns to normal performance levels (production, services, fill rate, etc.). Companies can develop resilience in several ways: increasing redundancy, building flexibility, and changing the corporate culture. The first has limited utility; the others are essential" (Sheffi 2005). While "bouncing back" is explicit in this definition, we also should be aware of the disruptions that necessitate the bouncing back. While natural disasters are the most noticeable, other human-related events also may cause disruptions to supply chains. Recent examples here include fires caused by negligence and surges in customer demand.

Perhaps the most widely used definition of sustainability was developed in 1987 by the Brundtland Commission (formally known as the World Commission on Environment and Development (WCED). It states that sustainable development, "meets the needs of the present without compromising the ability of future generations to meet their own needs." This definition focuses on the environmental dimension, which while critical to all businesses, limits how businesses today view sustainability. Augmenting the sustainable development concept in business is the concept of the triple bottom line (TBL), which considers the economic, environmental, and social dimensions of a business. Many companies report not only their economic results, but also metrics measuring environmental progress (e.g. tons of waste sent to landfills, energy consumption, amount of product recycled, and CO_2 emissions) and efforts regarding corporate social responsibility.

We will apply TBL concepts to supply chain resilience. As we will see, each of the three above-mentioned categories fosters supply chain sustainability. While not critical to our discussion here, we note the relevance of concepts of Resource Dependence Theory (RDT) (Pfeffer and Salancik 1978), which examines how organizations depend on external resources (e.g., material, managerial) that affect the organization's behavior. Moreover, how these resources are procured and managed is central to how the external resources of organizations affect the behavior of the organization. The procurement of external resources is an important tenet of both the company's tactics and strategies, and for supply chains, is a critical success factor.

The following sections discuss supply chain resilience and supply chain sustainability separately, and then link the two and discuss how effective strategies to achieve resilience are congruent with those fostering supply chain sustainability efforts. We then compare commonalities of supply chain resilience and sustainability with quality management and discuss how concepts in quality management can be used to frame discussions involving supply chain resilience and sustainability. Finally, we draw on these findings and discuss how they can be used by supply chain management practitioners.

2 Discussion

2.1 Supply Chain Resilience

As noted, a resilient supply chain is one that can bounce back from a disruption. The bouncing back process involves various states, including steps taken before known possible disruptions occur, steps taken to mitigate the damage of the disruption, and steps taken to fully recover. An extensive literature exists regarding supply chain resilience (see Zsidisin and Wagner 2010; Zsidisin and Ritchie 2009; Martin and Peck 2004; Chen et al. 2013; Munoz and Dunbar 2015; Pettit et al. 2010) and the concept of resilience supply chains has been made all the more visible with recent events regarding, tsunamis, hurricanes, earthquakes, factory fires, and market disruptions.

Although natural disasters first come to mind when thinking about supply chain disruption risks, other risks also exist. Drawing on some ideas in Fiksel (2003), we will categorize disruption risks in three categories: systemic, environmental, and social. Since each of these three "titles" are broad and may be defined differently in other contexts, their definitions in our context are as follow:

- Systemic: Risks related to the supply chain itself, the resources supporting it, and the related infrastructure. Examples would include poor supply chain design resulting in single points of failure, insufficient capacity to meet product delivery deadlines, unforeseen customer demand, incompetent suppliers and logistical partners (e.g., as regards timeliness, quality, safety), strikes, logistical delays, spikes in resource prices such as oil, changes in customer preferences, inability of infrastructure capacity (air, rail, water, electrical) to support production and delivery, and general managerial deficiencies causing mismatches between demand and supply.
- Environmental: Risks related to the natural environment and how it affects the supply chain. Examples include hurricanes, earthquakes, fires, tsunamis, heat waves, power outages, depletion of raw material resources, cold spells, snow, solar eruptions, and volcanoes, and their aftermath. Although many of these risks result in events that impact the system and might be confused with systemic risks, the difference is that systemic risks are those that occur "internally" and exclude those caused by the natural environment.
- Social: Risks related to social and organizational systems that are external to the firm. Examples include political risks such as changes in trade agreements, government and international organization regulations and guidelines, nongovernmental organization (NGO) campaigns, uprisings, wars, use of child labor, mistreatment of workers in factories, and adverse responses from local communities.

Three resiliency strategies mentioned by Sheffi (redundancy, flexibility, and corporate culture) provide a general framework to address these risks by considering specific examples in a strategy-risk combination grid. Given the large number of possible occurrences, drawing from the supply chain literature (including Fiksel 2003) and supply chain practices, we present some examples of practices that address the various combinations of supply chain risks and resiliency strategies. These are discussed in Fig. 1.

The examples in Fig. 1 illustrate how supply chain resilience requires managing multidimensional risks and calls for strategies that cross disciplines, and that range from the technical to the economic to the political. Global supply chains have increased the complexity of this process. Ensuring supply chain resilience involves monitoring and managing both physical, human, organizational, and social resources

FIGURE 1: SUPPLY CHAIN RISKS AND RESILIENCE STRATEGIES

Supply Chain Risks	Supply Chain Resiliency Strategies: Redundancy	Flexibility	Culture
Systemic	Use multiple suppliers; employ buffer inventories; configure multiple warehouses; employ product production capacity a multiple facilities	Use modular product design; standardize products; share information along the supply chain; respond to demand via capacity and production flexibility	Enhance communication with suppliers and customers; distribute power; establish a team culture; foster long term relationships; train vendors; act on customer feedback
Environmental	Avoid locating plants in high risk areas; employ redundancy in business continuity plans; avoid single raw material sources	Be able to shift production from plants located in high risk areas; employ multiple links in infrastructure networks; foster flexibility in business continuity plans	Enhance communication with suppliers and customers; establish a team culture; practice responding to disasters; foster long term relationships; establish links with customers
Social	Ensure all suppliers follow laws and codes of conduct; monitor suppliers; monitor political and other risks; give back to local communities	Maintain ability to switch quickly among suppliers; be able to effectively respond to changes caused by political and other risks; maintain a flexible workforce	Enhance communication with governmental agencies and NGOs; establish links with communities; establish a "good practices" culture among all suppliers

Fig. 1 Supply chain risks and resilience strategies

in an environment that is constantly evolving along technological, economic and political dimensions. Summarizing cases from Fig. 1 (and others not mentioned) leads to four general managerial strategies and practices:

- *Actively manage known economic and other risks.* This includes avoiding single points of failure throughout the supply chain, such as relying on one supplier, or relying on multiple suppliers, all of which are vulnerable to a single event. On the product side, it encourages modular product design and the ability to shift production among various product types depending on demand changes. It also involves managing known political and environmental risks.
- *Communicate within and without the supply chain*. This includes communications with suppliers (including those below Tier 1) and also customers. Outside the supply chain, communication includes governments, NGOs, and local communities. Facilitating communication involves adopting leading edge information technologies and fostering organizational relationships within and outside the supply chain.
- *Encourage good practices*. Supply chains that abuse labor and occupational safety laws, allegations of abuse of child labor laws, that foster environmental depletion such as overfishing, and that engage in political corruption are vulnerable to shocks which reduce their resilience.
- *Constantly monitor supply chain architecture*. Resilient supply chains depend on having the right architecture, not only for the present but also over time. Just as a building's design may become obsolete, to ensure resilience a supply chain's architecture must be assessed and revised based on evolving supply and demand realities. Resources affecting the architecture are not only physical resources such as factories, roads, and ships, but also less tangible resources such as supplier and customer relationships, relationships with logistics providers, and capabilities related to working under regulatory constraints.

2.2 Supply Chain Sustainability

Thinking about sustainability in business goes beyond just focusing on environmental factors and also includes economic and social factors. This is referred to as the triple bottom line (TBL). Many organizations report on all three factors, using evolving TBL metrics. Moreover, standards organizations, such as the International Standards Organization (ISO), have implemented many sustainability-focused standards (ISO 2017). Examples include: ISO 14001 Environmental Management; ISO 20400 Sustainable Procurement; ISO 26000 Guidance for Social Responsibility; ISO 45001 Occupational Health and Safety; ISO 50001 Energy Management; and other specific guidelines such as those for food safety, water quality, greenhouse gases, and intelligent transport systems.

Three drivers for sustainability in supply chains map to the three TBL dimensions:

- Economic: Sustainability can save money. At its heart, sustainability involves reducing waste. Examples include recycling and reverse logistics; optimizing logistics routes; consolidating shipments; reducing packaging, and reducing energy consumption costs.

- Environmental: Many waste reduction steps that save money also are environmentally friendly. In addition, sustainable behavior preserves natural capital, such as navigable waterways, clean air, biodiversity, and usable land. Natural capital may not appear on a corporation's balance sheet but may be critical to a corporation that uses it because it facilitates, and often is necessary to, business operations.
- Social: Sustainable behavior helps a company's stakeholders, such as workers, local communities, and stockholders. Moreover, as people become more environmentally conscious, customers are demanding more sustainable behavior from companies that provide their products and services.

Given these forces, Fig. 2 contains examples of performance indicators or metrics related to sustainability. Many of the examples given are informed by those discussed in Fiksel (2003).

Figure 2 illustrates how following sustainable practices affects supply chain behavior along many dimensions. Global customer and governmental concerns over sustainability issues have put business and supply chains in the spotlight and have raised questions about performance related to good practices, as illustrated in the ISO guidelines and other standards. Examples of many of the performance indicators mentioned in Fig. 2 fall in three categories:

- *Managing business costs*. These include direct economic costs like material, labor, and distribution costs inherent on the product production and delivery system. Also included are indirect costs related to workplace safety, warranty costs, recycling, and brand perception.
- *Managing natural capital and resource availability*. These go beyond the costs many think of and include resources in the natural environment that the firm depends on. Examples include: Waterways, air, forests, river deltas, fish populations, and stable environments for business operations and supply chain viability.
- *Fostering relationships*. These include relationships with customers, employees, communities, governments, investors, and NGOs. Implicit in the relationship is concern for both parties' well-being and adherence to sustainable practices.

A resilient supply chain that is not sustainable, in the TBL sense of the definition, itself is an unsustainable concept. There is a great deal of congruence with elements related to sustainable behavior when one thinks of how events impact supply chains and affect their resiliency. This relationship is discussed more fully in the next section.

2.3 Resilience and Sustainability

Resilient supply chains and sustainable supply chains have many common success factors. Rather than viewing sustainability as a "brake" to achieving supply chain resilience, sustainability can foster supply chain resilience in three ways. First, sustainable supply chains avoid many shocks that can disrupt supply chains and threaten

FIGURE 2: SUSTAINABILITY PERFORMANCE INDICATORS

Triple Bottom Line Category	Performance Indicator (Metric): Direct	Indirect	External
Economic	Raw material, labor, capital and operating costs; recycling revenue; costs for product disposal; business interruption due to natural disasters	Employee injury costs; warranty costs; customer retention costs; business interruption due to stakeholder intervention	Ecosystem productivity losses; resource depletion costs; government fines and interventions; consumer boycott costs due to NGO and other campaigns and interventions
Environmental	Product and packaging costs; hazardous materials used; energy consumption; material recycled; material sent to landfills; supply chain disruption costs from natural disasters	Product disposal liabilities; surface water runoff; smog creation; adverse affects on product or service brand image	Reduction in biodiversity; new and more stringent regulations; potential weather-related events such as forest fires
Social	Availability of product or service; employee satisfaction; image with investors; illness and mortality reductions; reduction in lost time injuries; increases in health and wellness	Reduction in employee risk; perception of the product or service brand; maintaining supplier base	Relationships with governmental agencies and NGOs; links with communities; links with potential customers and investors; links with media

Fig. 2 Sustainability performance indicators

supply chain resilience. This avoids the need to trigger business continuity plans and saves financial and other resources. Second, when events do occur that threaten a supply chain's viability, following good sustainability practices can foster a return to normal operations by marshaling economic, human, and political resources. These good practices also facilitate having more robust business continuity plans. Third, when shocks to the supply chain occur, employing a sustainability mindset can create goodwill among customers and other stakeholders, which can enhance the firm's brand and can develop long term loyalty. A resilient supply chain whose products are abandoned by its firm's customers is not a desired outcome.

Figure 3 presents linkages between supply chain resilience and supply chain sustainability. In it, the observations at the end of each of the above two sections constitute the row and column titles. We developed the observations mentioned in

FIGURE 3: THE RESILIENCE - SUSTAINABILITY RELATIONSHIP

		Sustainability Category		
		Managing Business Costs	**Managing Natural Capital and Resource Availability**	**Fostering Relationships**
Resilience Category	**Risk Management**	Manage costs while managing risk; this includes identifying and managing indirect costs and highlighting the cost implications of shocks that can impact supply chain resiliency.	Monitor status of natural capital needed for ongoing operations and identify how changes in natural capital may create risks to the supply chain; when appropriate, develop amelioration strategies	Develop good relationships which can help identify to risks, to foster resilience when risk events occur, and to ensure that external organizational support is in place when needed.
	Coordination	Manage the costs of the technologies and time needed to foster relationships, to share information, and to provide consulting services to supply chain partners.	Communicate natural capital and resource status to supply chain partners, governments, and outside organizations. Develop programs to ensure that sufficient natural capital resources are available to support firm operations.	Foster relationships and implement coordination practices to foster supply chain resilience and sustainable operations. This involves relationships with supply chain partners, governments, and outside organizations.
	Good Practices	Implement and manage in a cost effective manner, programs to monitor and continuously improve good practices related to employees and business operations.	Develop links between the firm and external organizations to ensure that the firm's business practices do not threaten the natural capital, and that the resources needed to maintain a resilient supply chain exist.	Foster relationships and practices with workers, suppliers, business partners, governments, and relevant external organizations, that are needed for good business practices to be effective
	SC Architecture	Develop metrics to measure and manage costs in existing architectures, and which can be used to evaluate the cost implications of new, alternative architectures.	Ensure that the SC architecture does not create conditions that cause environmental degradation, diminution of natural capital, or foster human capital abuses.	Establish relationships to ensure that the SC architecture includes effective processes with workers, suppliers, business partners, governments and relevant external organizations

Fig. 3 The resilience-sustainability relationship

the grid by considering strategies mentioned from the literature and from ongoing good practices.

The relationship between supply chain resilience and sustainability is illustrated by four resilience categories (Risk Management, Coordination, Good Practices, and Supply Chain Architecture) and three TBL categories (Managing Business Costs, Managing Natural Capital and Resource Availability, and Fostering Relationships). Using this framework, efforts to manage supply chain resilience often depend on the following sustainable supply chain practices; the two concepts are mutually supportive.

Supply chain resilience and sustainability can be viewed through a lens similar to the one employed for quality management. Past critics of quality practices felt that, while perhaps a noble concept, achieving higher quality meant incurring higher costs. In the same vein, some critics of business sustainability claimed that following TBL practices increased costs and reduced profits. Implicit in this critique, was that sustainability requirements created additional constraints that reduced supply chain options—for example, constraining a supply chain to use only "sustainable suppliers" could lead to single points of supply, capacity bottlenecks, or slower logistical responses.

For quality management, the concept of the "total cost of quality" is widely used (Omachonu and Ross 2005). The total cost of quality consists of four costs: Preventions costs, which include material costs and machine maintenance costs; Inspection costs, which include in-process inspections (such as maintaining control charts) and inspections prior to shipping the end product to customers; Internal Failure costs which include costs related to scrap and rework; and External Failure costs, which include warranty costs, return costs and indirect costs related to degradation of the brand and lost customers. The underlying logic behind quality management practices is that applying resources to the prevention and inspection categories results in lower internal and external failure costs. In this sense, money saved outweighs money spent, and thus quality management pays off.

A similar logic may apply to sustainability and supply chain resilience. Four resilience-sustainability cost categories are:

- *Operational Costs*—the ongoing costs of the incremental sustainability-related decisions incurred when managing a supply chain. These include costs related to personnel, supply chain architecture (including information systems), product design, procurement, and distribution costs. They involve all the marginal costs related to time expended and other resources explicitly used, with the purpose of implementing sustainable practices that enhance a supply chain's resilience.
- *Compliance Costs*—the costs of adhering to good practices, including codes of conduct for suppliers, and which also include auditing suppliers and meeting environmental and labor restrictions in all venues that comprise the supply chain's geography. As above, these would include costs of personnel and other resources used in the compliance effort.
- *Direct Event Costs*—the direct costs to the firm from its suppliers and customers when a "resilience event" occurs, calculated with and without following sustainability-related business practices. These costs would include the costs to bring the organization back to a normally agreed on level of functioning. They also would include the immediate costs of dealing with events such as fires, earthquakes, using underage labor, capacity shortages and customer costs such as immediate lost business and lawsuits. Hopefully, implementing more sustainable practices would reduce direct event costs, relative to a base case where non-sustainable

practices would be used. The difference reflects the benefits of following sustainability-related practices.

- *Indirect Event Costs*—the costs that impact the firm later, due to the resilience event. These would include lost customers and lost future business, relevant warranty costs, fewer suppliers wanting to deal with the firm, a loss of attractiveness to future employees, and a diminution of the firm's brand. As with the direct event costs, these costs would be marginal costs (or actually savings) relative to a base case where non-sustainable practices would be used.

The total resilience-sustainability cost metric provides with an organization the opportunity to quantify sustainability-related costs supporting supply chain resilience. Considering both visible and hidden costs helps incorporate sustainable practices into supply chain resilience decisions and create more robust supply chain resilience solutions.

2.4 Relevance to Practice

The above ideas can be used to develop approaches that supply chain practitioners can use to address the specific resilience-sustainability challenges that they encounter. One area involves using the previous section's cost categories to evaluate alternative supply chain joint resilience and sustainability strategies. Examples would include examining alternative architectures, analyzing the impact of changes in regulations, or developing alternate sourcing criteria. Other areas involve extending ongoing efforts in risk and inter-organizational communication to address the resilience and sustainability nexus.

Cost Management

Cost management involves considering operational, compliance, direct, and indirect costs mentioned above, as tailored to meet the specific needs where resilience and sustainability meet. Examples of actions include:

- Developing metrics to measure and manage resilience-sustainability costs in existing architectures, and to evaluate the cost implications of new, alternative architectures;
- Identifying and managing indirect sustainability costs, and highlighting the cost implications of shocks that can impact supply chain resiliency;
- Managing the costs of existing and new technologies and fostering links necessary to share information and to provide consulting services to supply chain partners.

Risk Management

Risk management involves extending current practices to include risks created by the resilience-sustainability nexus and to ensure that in their analyses, managers consider "less examined" risks such as those regarding natural capital and good sustainability practices. Examples include:

- Monitoring the status of natural capital needed for ongoing operations, identifying how changes in natural capital may create risks to the supply chain, and developing and/or supporting programs and policies to ensure that sufficient natural capital resources are available to support firm operations;
- Implementing and managing programs and policies to monitor and continuously improve good practices related to sustainability and how these practices affect risk exposure, employees, and business operations;
- Ensuring that the supply chain architecture does not create conditions that cause environmental degradation, diminution of natural capital, decline in workplace safety, or foster human capital abuses.

Relationship Management
Relationship management involves extending ongoing efforts involving suppliers and customers to include resilience and sustainability dimensions, as well as to better foster relationships with external agencies and organizations such as governments, trade organizations, international organizations, and NGOs. Examples include:

- Developing relationships with suppliers, business partners, governments and other organizations to help identify risks, foster resilience, and ensure that external organizational support is in place when needed;
- Communicating to supply chain partners, governments, and outside organizations, the status of natural capital and other resources needed for effective supply chain operations, to ensure that the firm's business practices do not threaten the natural capital and other resources needed to maintain a resilient supply chain;
- Fostering relationships and practices with workers, suppliers, business partners, governments, and relevant external organizations that are needed to ensure that good business practices are effective, robust, and ensure that the supply chain architecture creates processes meets the current and future needs of the organization.

3 Conclusion

Just as customer expectations help define what is a quality product, so do customer and market expectations define a resilient supply chain. The "bouncing back" definition given above indicates that the bouncing back needs be done quickly and completely. Moreover, these time and completeness requirements grow more rigid over time. Just as requirements for supply chain resilience grow greater, so do those for supply chain sustainability. As with resilience, customer and market expectations have increasingly pushed supply chains to become more sustainable, not only along the environmental dimension, but also along economic and social responsibility dimensions.

As noted above, sustainable and resilient supply chains are linked in three ways: reducing shocks; returning to normal sooner; and creating stakeholder goodwill. Rather than being viewed as a cost that may not be justified economically, sustainability should be viewed as a necessary element of the solution and an enabler of supply chain resilience. This is especially true when considering total incurred costs.

Just as sustainable supply chains foster resilience, so do resilient supply chains foster sustainability. Regardless of the TBL metric, one chooses—economic, environmental or social—non-resilient supply chains degrade TBL performance. Certainly, this is true for economic performance, where lack of resilience results in short- and long-term economic losses. Supply chains that cannot bounce back also create barriers to environmental performance. First, they illustrate managerial flaws underlying the entire enterprise, which are flaws that also leech over into environmental management and may lead to cutting corners when faced with environmental issues. Second, they create the possibility of lurching from one resilience crisis to another, which makes planning—including planning for improved environmental performance—more difficult. Finally, non-resilient supply chains harm social performance regarding primary and secondary stakeholders of the firm because resources (economic and managerial) are diverted or unavailable.

Resilient and sustainable supply chains do not need to result in zero-sum type trade-offs, but rather are mutually reinforcing, and go hand-in-hand. Although the definition of sustainability given above is environmentally focused, a second definition involves an entity that is capable of being sustained at some level or upheld—a definition very similar to that of resilient. Though they appear to be different, a sustainable supply chain is resilient, and a resilient supply chain is indeed, sustainable.

References

Chen, J., Sohal, A. S., & Prajogo, D. J. (2013). Supply chain risk mitigation: a collaborative approach. *International Journal of Production Research, 57*(1), 2186–2199.

Fiksel, J. (2003). Designing resilient, sustainable systems. *Environmental Science and Technology, 37,* 5330–5339.

International Standards Organization (2017). Retrieved October 27, 2017, from https://www.iso.org/popular-standards.html.

Martin, C., & Peck, H. (2004). Building the resilient supply chain. *The International Journal of Logistics Management, 15*(2), 1–14.

Munoz, A., & Dunbar, M. (2015). On the quantification of operational supply chain resilience. *International Journal of Production Research, 53*(22), 6736–6751.

Omachonu, V. K., & Ross, J. E. (2005). *Principles of total quality* (3rd ed.). New York: CRC Press.

Pettit, T. J., Fiksel, J., & Croxton, K. L. (2010). Ensuring supply chain resilience: Development of a conceptual framework. *Journal of Business Logistics, 31,* 1–21.

Pfeffer, J., & Salancik, G. R. (1978). *The external control of organizations: A resource dependence perspective*. New York: Harper and Row.

Sheffi, Y. (2005). Building a resilient supply chain. *Harvard Business Review*. Retrieved January 3, 2018, from http://web.mit.edu/sheffi/www/selectedMedia/genmedia.buildingresilientsupplychain.pdf.

Zsidisin, G. A., & Ritchie, B. (2009). *Supply chain risk: A handbook of assessment, management and performance*. New York: Springer.

Zsidisin, G. A., & Wagner, S. M. (2010). Do perceptions become reality? The moderating role of supply chain resiliency on disruption occurrence. *Journal of Business Logistics, 31,* 1–20.

Chapter 16
Sustainability Risk Management in Supply Chain

Jukka Hallikas, Katrina Lintukangas and Daniela Grudinschi

1 Introduction

Sustainability and the responsibility to perform a firm's business without harming nature and people have become an important value for many companies. Today, it is widely acknowledged among practitioners and scholars that investments in sustainability may increase profit and business performance in terms of increased resource efficiency and the rise of new innovations in the long run (Nidumolu et al. 2009; Lindgreen and Swaen 2010). Ensuring sustainability is an essential dimension of a firm's risk management. In particular, sustainability risks arising from supply chains are a concern. News of environmental hazards or child labor harm a company's image and brand even when the incidents happen at supplier or sub-supplier sites. Therefore, the ability to ensure sustainability is based on a company's smart strategic management of the whole supply chain and strong risk management skills (Ghagde et al. 2012).

Sustainable development refers to considering and balancing the economic, environmental, and social impacts on the business activity (Elkington 1998; Goncz et al. 2007; Sikdar 2003). Although contributing to the organization's sustainable development is a collaborative effort by all of the organization's departments, assuring responsibility and transparency in the supply chain is the central task of purchasing and supply chain risk management (Schneider and Wallenburg 2012). Companies may put a lot of effort and commitment in implementing sustainability; however, many firms encounter serious difficulties while dealing with this issue (Lindgreen et al. 2009). Thus, more knowledge is needed regarding how sustainability can be implemented, controlled, and ensured in the business and the supply chain (Lee 2008).

J. Hallikas (✉) · K. Lintukangas · D. Grudinschi
Lappeenranta University of Technology, Lappeenranta, Finland
e-mail: Jukka.Hallikas@lut.fi

G. A. Zsidisin and M. Henke (eds.), *Revisiting Supply Chain Risk*, Springer Series in Supply Chain Management 7, https://doi.org/10.1007/978-3-030-03813-7_16

In this chapter, the implementation of sustainability practices and processes for assuring sustainability in the supply chain from the risk management perspective is clarified. The aim is to provide knowledge and solutions for managing sustainability risks in supply chains. The practices for managing sustainability risk in the supply chain are introduced and guidelines for including them in each stages of the procurement process. The process of implementing sustainability with risk management incorporated in the supply chain is described step by step.

Based on the empirical data obtained from interviews with supply chain managers and drawing on the sustainable supply chain literature, this chapter identifies the challenges of managing the implementation of a sustainable supply chain. Guidelines for supply managers regarding the process of implementing sustainability in the supply chain, as well as how risk issues should be managed during the whole process of implementing sustainability, are provided.

2 Sustainable Supply Chain

In recent years, sustainability and corporate social responsibility (CSR) have become key business issues and an important topic on research agendas. CSR is not a new concept. It was first proposed by Sheldon (1924) and later by Bowen (1953). In their books, they specify that every corporation must take responsibility for social problems. Carroll (1979) provided a widely adopted three-dimensional view of CSR: environmental, social, and economic. From a macroeconomic perspective, sustainability is defined as a "development that meets the need of the present without compromising the ability of future generations to meet their needs" (World Commission on Environment and Development 1987, p. 8). The microeconomic perspective of sustainability suggests that organizational sustainability consists of three main components: environment, society, and economic performance. This perspective is also similar to "the triple bottom line," introduced by Elkington (1998, 2004), which suggests that all three components (environment, social, and economic performance) must be balanced and considered simultaneously by organizations in their social responsibility activities.

According to Seuring and Müller (2008, p. 1700), sustainable supply chain management is "management of material, information and capital flows as well as cooperation among companies along the supply chain while taking goals from all three dimensions of sustainable development, i.e., economic, environmental and social, into account which are derived from customer and stakeholder requirements." Sustainability in supply chains is driven by several factors. Regulation and adoption of quality standards (Chen 2005), internal and external customers' expectations (Schneider and Wallenburg 2012) and company owners' values, and commitment of senior management (Giunipero et al. 2012) are the main drivers of a sustainable supply chain. Moreover, serious environmental and social challenges, such as climate change, limitation of material resources, food security, and exhaustion of energy sources, have deepened the need for companies to manage sustainability risks

(Clapp and Rowlands 2014). To promote sustainability, various initiatives through reporting have been taken. For example, the Global Reporting Initiative (GRI 2009) provides guidelines and encourages suppliers to report their social responsibility in order to increase supply chain transparency and sustainable procurement practices. Another initiative, the Global e-Sustainability Initiative (GeSI), collects and shares CSR data from key suppliers, with which organizations share ideas and best practices in CSR (Harwood and Humby 2008). The International Standards Organization (ISO) 14001 international standard for environmental management systems (EMSs) promotes external auditing and certification of compliance by an accredited certification body (evaluation by an independent third party). The ISO 26000 standard concentrates on social responsibility and ISO 20400.2 on sustainable procurement. The standardization sets targets to continually improve the environmental and social performances of firms and increase understanding of legal requirements and corporate and stakeholder obligations concerning sustainability management.

3 Sustainability Risks in the Supply Chain

Although numerous global initiatives for sustainability have been undertaken, implementation in supply chains has faced many challenges, because of the lack of knowledge and skills for tackling sustainability risks in supply management. Supply risks are serious incidents that may harm a firm's business and paralyze the whole supply chain. Supply risk is "the probability of an incident associated with inbound supply from individual supplier failures or the supply market occurring, in which its outcomes result in the inability of the purchasing firm to meet customer demand or cause threats to customer life and safety" (Zsidisin 2003, p. 222). Christopher et al. (2011, p. 67) defined supply risk as the risk of being "associated with the sourcing of products by a focal firm." It is widely acknowledged that sustainability risks are connected strongly with supply chain and supplier management (see, e.g., Foerstl et al. 2010; Ghagde et al. 2012). Especially in terms of a company's image and brand value, sustainability risks in global sourcing and outsourcing of company functions to low-cost countries and how to manage and mitigate risks in these circumstances have been studied (Christopher et al. 2011). Moreover, violations of property rights, unsatisfactory quality of the materials or services, volatility of prices, and rises in costs are supply risks companies face frequently (Holweg et al. 2011).

Hofmann et al. (2014) defined sustainability-related risk as "a condition or a potentially occurring event that may provoke harmful stakeholder reactions" and as "a sustainability risk within a focal firm's supply chain." According to Multaharju (2016), companies should gain specific capabilities for managing sustainability-related risks arising from the supply chain. Collaboration and the ability to control a supplier's sustainability, stakeholder management, sustainability risk mitigation practices, and collaboration and orientation toward supply chain sustainability are essential elements of sustainability risk management.

Risks can occur in several stages of a supply chain. According to Manuj and Mentzer (2008), risks can be supply risk (supplier selection and control), operation risk (production failures and process breaks), demand risk (changes in customer preferences and fluctuation in sales), and security risk (product fraud and leaks of business secrets). Moreover, risks can happen at various levels in the supply chain. Macro-level risks include political and government, macroeconomic, legal, social, and natural risks. Meso-level risks are, for example, finance, design, and operation risks, and micro-level risks concern business relationships and third-party risks (Bing et al. 2005). Zsidisin (2003) divided supply risks into the sources of the risks and the outcomes following the risk incidents. Table 1 summarizes the main risk types and the possible consequences of the risk incident and provides examples of sustainability-related risks.

The complexity of managing risks in supply chains increases exponentially when sustainability dimensions are included (Dai and Blackhurst 2012). Controlling sustainability at every level or phase in a supply chain is extremely challenging because a firm may not have the power or possibility to influence other parties in a chain. Therefore, from the risk management perspective, including sustainability aspects in planning of the sourcing, procurement policies, supply market analysis, and specifications of the products are essential.

Table 1 Summary of sustainability-related supply risk types

Sustainability risk types	Sustainability-related risk examples	Possible consequences	Authors
Conflict of property rights	Product fraud, theft of business secrets	Loss of intangible assets, ownership disputes regarding innovation	Hallikas et al. (2005)
Damage to company reputation	Pollution, child labor, corruption	Loss of sales, decrease in equity	Simpson and Power (2005)
Unsatisfactory quality of purchases	Low wages, lack of training, unknown origin, increase in waste	Increase in after-sales costs, product recalls	Christopher et al. (2011)
Rise in purchasing price and costs	Lack of capable suppliers and scarce resources, investments in cleantech, price of energy	Decrease in margin, volatility of prices	Holweg et al. (2011)
Outsourcing of critical activities	Loss of control of the production and transparency of the supply chain	Loss of capability, increased dependence on suppliers	Lonsdale (1999)

4 Risk Management in a Sustainable Supply Chain

The objective of risk management in the context of sustainable procurement is to identify, prioritize, and manage internal and external risks (including opportunities) related to procurement activities dynamically and by adapting to changing conditions. The ISO 20400 standard for sustainable procurement provides understanding of sustainable procurement, sustainability considerations, and implementation of sustainable procurement. According to ISO 20400, the sustainability objectives of the procurement policy and strategy should be transformed into operational priorities for the procurement function through risk management. What is essential is that the sustainability considerations in procurement are driven by company policy and strategy. Here, the commitment to the sustainability, sustainability targets, and resources is defined.

Risk assessment and risk treatment are the core of risk management. Risk assessment includes identification of the risks, analysis of the probability, and evaluation of the severity of the risk. Risk treatment is a strategy or tactic for mitigating or removing the risk. According to ISO/DIS 20400.2 standard, companies should identify short-, medium-, and long-term sustainability risks, assess their criticality for the company, and apply procurement practices to treat sustainability risks. Consequently, the sustainability objectives of supply management need to be transformed into operational priorities and connected to risk management by utilizing different approaches, such as categorizing products and suppliers across sustainability targets. Table 2 shows practices for managing operational risk to apply during the sourcing planning phase.

Table 2 Operational risk management practices to apply during sourcing planning

Planning of supply process	Sustainability risk management practices
Supplier collaboration	Supplier assessment
	Proactive interaction and information change
	Communication of policies and code of conduct
	Contracts
	Monitoring and measurement
	Supplier relationship management
Specification of the product or service	Sustainability criteria setting
	Regulation and limitations
	Resource efficiency and innovations
	Examination of substitutes and other options
	Identification of cost structure
Operations	Roles and tasks of actors in the supply chain
	Control and follow-up

Adapted from ISO 20400

Priorities for different sustainability aspects can be set by assessing the risk impact of different sustainability areas which can be found, for example, in ISO 20400 standard. These sustainability areas can be prioritized by showing which sustainability areas require the most attention in a purchasing situation. See the example sustainability areas and action points in Table 3. The priorities are usually set according to purchase categories or may be part of supplier management. The traditional risk assessment framework which takes into account the impact and likelihood of risks may also be applied here. The sustainability risk impact assessment should integrate sustainability considerations in each purchasing category by focusing on the sustainability areas that are most critical for the company's supply chain.

After the sustainability areas of the purchase have been prioritized, the next step is to integrate sustainability in the procurement process. The procurement process

Table 3 Action points and their priorities for risk management activities

Supply governance and decision making	Human rights	Labor practices	The environment	Fair operating practices	Consumer issues	Community involvement and development
Develop a procurement policy that reflects a commitment to sustainability	Identify the risks of human rights	Ensure that labor issues are addressed	Prevent pollution	Prevent corruption in collaboration with suppliers	Provide fair marketing, factual and unbiased information, and fair contractual practices	Contribute to community involvement and education
Apply the principles of sustainable procurement to procurement activities	Alert the procurement function about the supply of goods or services from areas of conflict in human rights	Ensure good working conditions are provided	Use sustainable resources	Support and promote fair competition between suppliers throughout the supply chain	Protect consumers' health and safety	Consider helping to develop or improve skills development programs in the community
Allocate sufficient resources to the implementation of sustainability practices	Apply practices of civil and political rights	Contribute to the development and maintenance of occupational health and safety systems	Mitigate and adapt to climate change	Promote social responsibility throughout the supply chain	Stimulate the design of products and packaging so that they can be easily used, reused, repaired, or recycled	Consider the positive impact of sustainable purchasing decisions, using local suppliers, on employment creation for SMEs
Identify, prioritize, and manage internal and external risks related to the procurement activities	Apply practices of economic, social, and cultural rights	Contribute to providing workers with access to skills development	Protect the environment, biodiversity, and restoration of natural habitats	Demonstrate respect for property rights	Provide information about goods or services, including country of origin, energy efficiency, contents, or ingredients	Contribute to development of and access to technology in local communities

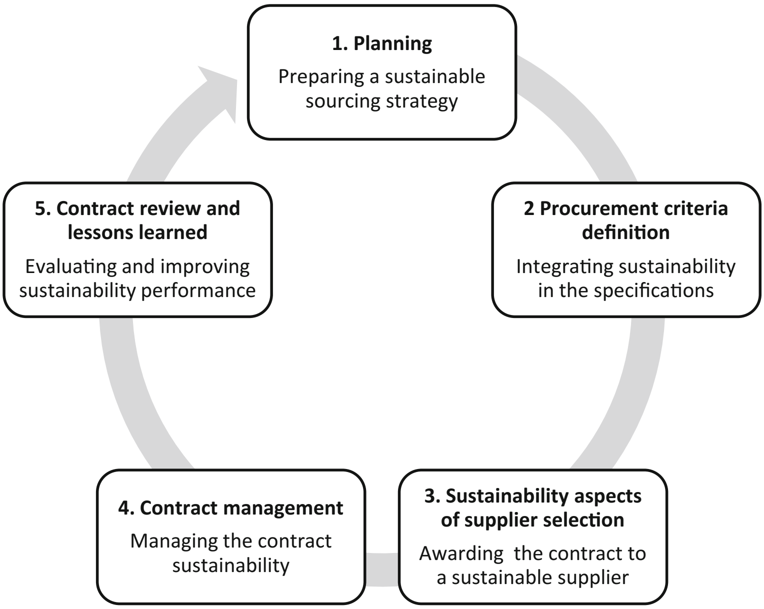


Fig. 1 Integrating sustainability in the procurement process (adapted from ISO 20400)

steps are illustrated in Fig. 1. The task is to determine how each process step can incorporate sustainable procurement practices. In the planning stage, the sourcing strategy is prepared and defined. The procurement criteria definition stage integrates sustainability into the procurement specifications. The next stage in the process incorporates sustainability aspects in selecting and contracting suppliers. The contract is managed during the contract management stage taking into account the sustainability aspects. The contract review and lessons learned phase evaluates the sustainability performance and improvement practices for the following actions.

Based on ISO 20400, the following are examples of the practices of the different purchasing process stages:

1. **Planning**—Integrate sustainability into the sourcing strategy by addressing the considerable sustainability risks and life cycle costing (LCC), analyzing the organizational needs, and analyzing the supply markets.
2. **Criteria definition**—Define the procurement criteria to clearly reflect the priorities defined in the procurement strategy, for example, the physical, performance, and functional requirements. Include clauses that enable the organization to increase its control over what happens in the supply chain.
3. **Supplier selection**—Select suppliers based on sustainability principles, practices, and performance.
4. **Contract management**—Communicate sustainable elements and associated performance targets by relevant stakeholders. Establish a contract management

plan that reflects the organization's sustainability objectives and related key performance indicators.

5. **Contract review**—Communicate details about the achievement of sustainability objectives, targets, and occurred risks contained in the contract. Learn from the past performance and review the priorities and objectives to promote continual improvement.

5 Case Examples of Sustainable Supply Chain Risk Management

In the following section, we identify and analyze sustainability practices in different case organizations representing various industrial sectors. Each organization was committed to the study and allowed focus group sessions to be organized for the selected experts in the purchasing, supply management, and sustainability risk management fields. A total of 56 persons participated in the focus group interviews. Sessions were supported by a group decision support platform that automates and streamlines the group interview process. Each group session lasted for approximately two hours. The participants were asked about the practices that are implemented to assure and manage risk in sustainability of purchasing and supply. More than 200 different methods, tools, and policies for sustainable assurance and risk management of the supply chain were identified during the sessions. They were grouped in categories according to the general phases in the purchasing process and for the generic development category which outlines the quality assurance, supplier development, and improvement activities. The main results of the findings are presented in the following.

5.1 Requirements for Responsibility in Purchasing

The organizational requirements for sustainable purchasing assurance and risk management were identified during the group interviews. The main requirements were related to supplier management and relationships, visibility in the supply chain, cooperation and networking, knowledge of the business environment, ethical behavior and law, and processes for executing sustainability.

Processes for managing supplier relationships seem to be the key area where sustainability assurance takes place. Supplier selection, contracting, and supplier development are the phases where sustainability and visibility in the supply chain are built. Internal and external cooperation and networking are essential to share knowledge and develop standard methods for handling sustainability issues in purchasing and supply. In-depth understanding of the business sector, products, production environments, cost breakdown structures, and people in the business facilitates the proper management of sustainability. Ethical considerations were also given special attention among the participants. Deep understanding of the principles of sustainability and ethical behavior in the organization and in the suppliers in the supply chain was remarked as an important requirement of sustainability. Finally, the functional processes must assure the implementation of sustainability in the purchasing and supply chain.

5.2 The Process of Responsibility Assurance in the Supply Chain

Based on the data gathered from the focus group interviews, the following stages were identified for the process of assuring responsibility in the supply chain.

a. **Strategic planning**: The first step in the process of assuring responsibility is strategic planning. First, the sustainability goal must be set, which includes specific objectives for reaching the main goal. Involving suppliers early in the planning process (Dou et al. 2014) and maintaining good relationships with customers are essential for successful planning. Through good collaborations with customers and suppliers, planning for how to use new forms of energy, how to use materials or energy efficiently, or how to find new efficient transportation, solutions can be achieved. The procurement process must be planned carefully with detailed specifications, which allow responsibility options to be included in the bidding process. Roles must also be well defined during strategic planning.
b. **Supplier assessment and supplier selection**: To implement sustainable procurement, the whole supply chain must meet the sustainability criteria (Manuj and Mentzer 2008). Suppliers that meet the sustainability criteria, or which are eco-labeled, must be selected for this purpose. Before the best suppliers are selected, a broad and detailed supplier assessment must be performed. The assessment includes information and surveys on the minimum requirements related to product quality (proprieties and the production process) and responsibility issues (environmental and social). In addition, asking about supplier references and responsibility certificates helps select the appropriate suppliers.
c. **Contracts with suppliers**: After the supplier selection process, the contracts must be written. The contractual policies must be specified in detail, and wide documentation of contracts must be provided (Basmadjian et al. 2015). The policies must include responsibility issues, code of conduct, product quality requirements, and subcontractor requirements. In addition, sanctions regarding contract violations must be stipulated in the contracts. For recognized responsible suppliers (which are already eco-labeled), long-term contracts are recommended.
d. **Monitoring and measuring**: In order to assure responsibility in the supply chain, a continuing monitoring mechanism of suppliers during the whole contract period must be organized (Gallardo-Vázquez and Sanchez-Hernandez 2014). This includes supplier audits and various responsibility metrics (e.g., energy

efficiency and carbon dioxide emissions for every product). Ethical issues must be highlighted in supplier feedback. Moreover, applying penalties if the requirements are not met and rewarding good suppliers are important instruments when the aim is to assure responsibility.

e. **Supply development and assurance**: Based on the evaluation during the monitoring and measuring process, supply development and assurance require new actions and better approaches to meet the sustainability criteria. Effective development can be assured through collaborations with suppliers (Dou et al. 2014) that are based on transparency and trustful relationships. Much effort should be put into trust-building instruments and collaborative practices (e.g., education and training, redesigning the procurement process, or re-evaluating efficiency requirements) which will increase supplier commitment and responsibility.
f. **Cooperation and networking**: To be able to achieve the objectives and to continue to develop the supply chain for better responsibility, effective cooperation and networking at many levels must be established (Brito et al. 2014). Continuing internal cooperation with all organization employees, as well as external cooperation and networking with external stakeholders and officials, can provide new information and new knowledge needed to assure responsibility. Regularly organized in-house meetings, which handle responsibility issues, can have a big impact on the commitment to responsibility at all organization levels. Additionally, participating in supplier forums and networking events or being actively involved in the stakeholders' industries provides organizations with new knowledge but also can contribute to involving other external stakeholders in responsibility issues.

5.3 *The Role of Risk Management in Assuring Responsibility in the Supply Chain*

Based on the cases, the most important risk management issues and practices that must be considered in the process of risk management for assuring responsibility are illustrated in Table 4. The specified actions should be taken in managing risk management to assure better responsibility in the supply chain. Every risk management action is attributed to a specific phase of the purchasing process. It follows that the role of risk management during the whole process can be easily observed.

In the last column of Table 4, how risk actions are assessed during different stages of the responsibility implementation process can be perceived. During all stages of the responsibility implementation process, risk issues must be managed to assure responsibility. Furthermore, strategic planning and supplier development (stages a and e, respectively) connect most risk management actions. During the responsibility implementation process, both stages take place in close collaboration with suppliers. Therefore, risk management plays a very important role during the whole responsibility implementation process.

Table 4 Linking risk management issues with the responsibility implementation process (*)

Risk management issues	Actions for assuring responsibility	Stages in the responsibility implementation process (*)					
		a	b	c	d	e	f
Building trust and open relationships with suppliers	Open dialog, regular feedback	x			x	x	
	Instruction on ethical issues					x	x
	Code of conduct	x		x			
	Supplier audits		x		x		
	Business review with suppliers					x	
Supplier commitment	Collaborating strategically with suppliers	x				x	x
	Training and educating suppliers					x	
	Developing new practices together with suppliers	x				x	
	Developing collaborative projects with suppliers	x				x	x
	Caring about supplier safety	x				x	
Classifying suppliers	Classifying suppliers based on responsibility criteria		x				
	Establishing minimum requirements		x	x			
Quality control and management	Quality standards and documentation	x		x			
	Test documentation, assuring products' traceability with stamps	x		x			
	Using risk management standard tools	x				x	
	Defining responsibility criteria for procurement	x	x				
Responsibility development and support	Training and educating suppliers					x	
	Supporting suppliers in taking responsibility	x					
	Defining responsibility by using examples	x					x
	Management support for responsibility	x				x	
	All staff commit to responsibility issues	x			x	x	x

(continued)

Table 4 (continued)

Risk management issues	Actions for assuring responsibility	Stages in the responsibility implementation process (*)					
		a	b	c	d	e	f
Procurement process development	Choosing the right procurement process	x				x	
	Assuring procurement process transparency	x			x	x	
	Procurement acquisition monitoring	x				x	
	Ecological procurement activity list	x		x		x	
	Efficiency requirements					x	x
	Procurement systems that support responsibility automation					x	
	Proactive procurement processes	x				x	x

*a—strategic planning, b—supplier assessment and supplier selection, c—contracts with suppliers, d—monitoring and measuring, e—supplier development and assurance, f—cooperation and networking

6 Discussion and Conclusions

This chapter provided insight into how responsibility can be implemented and assured in a sustainable supply chain and what role risk management plays in this process. Although sustainability and responsibility issues have grown in recent years (Greenfield 2004; Maignan and Ralston 2002; McWilliams et al. 2006; Pearce and Doh 2005), implementing responsibility in the supply chain has been reported to be challenging (Lindgreen et al. 2009). This chapter offers knowledge of the organization and integration of sustainability actions in the supply management process. Furthermore, the analysis shows that risk management plays a very important role during the whole responsibility implementation process, especially during the stages that involve close collaboration with suppliers (the strategic planning phase and the supplier development and assurance phase, respectively). These implications are likely to help the implementation of sustainable risk management in the supply chain in organizations.

This chapter provides insights into integrating sustainability in the procurement process. As observed in sustainability procurement standards (ISO 20400), it is necessary to have a systematic process for assuring responsibility during the procurement process phases. By developing and following standard processes and actions connected to the different phases of the procurement process, it is possible to manage implementation of sustainability properly. Appropriate frameworks help supply chain managers to understand the tools and processes used in purchasing for assuring a sustainable supply and the role of risk management while implementing social responsibility in the supply chain.

The illustrative case findings provide examples of practices for assuring and managing the risk of sustainability in supply chains. Although these practices can sometimes be regarded as sector specific, there are many actions and practices that fit most companies. The purpose of these practices is to identify and prioritize the most important sustainability issues the company faces and to implement the actions required to manage risks during the procurement process phases. This approach targets the risk management actions to all the supply management process phases. This is likely to bring more visibility and control to sustainable supply chains.

References

Basmadjian, R., Müller, L., & De Meer, H. (2015). Data centres' power profile selecting policies for demand response: Insights of green supply demand agreement. *Ad Hoc Networks, 25,* 581–594.

Bing, L., Akintoye, A., Edwards, P. J., & Hardcastle, C. (2005). The allocation of risk in PPP/PFI construction projects in the UK. *International Journal of Project Management, 23*(1), 25–35.

Bowen, H. R. (1953). *Social responsibilities of the businessman.* New Yorker: Harper and Row.

Brito, L. A. L., Brito, E. P. Z., & Hashiba, L. H. (2014). What type of cooperation with suppliers and customers leads to superior performance? *Journal of Business Research, 67*(5), 952–959.

Carroll, A. B. (1979). A three-dimensional conceptual model of corporate performance. *Academy of Management Review, 4*(4), 497–505.

Chen, C.-C. (2005). Incorporating green purchasing into frame of ISO 14000. *Journal of Cleaner Production, 13*(9), 927–933.

Christopher, M., Mena, C., Khan, O., & Yurt, O. (2011). Approaches to managing global sourcing risk. *Supply Chain Management: An International Journal, 16*(2), 67–81.

Clapp, J., & Rowlands, I. H. (2014). Corporate social responsibility. In J.-F. Morin & A. Orsini (Eds.), *Essential concepts of global environmental governance* (pp. 42–45). New York: Routledge.

Dai, J., & Blackhurst, J. (2012). A four-phase AHP-QFD approach for supplier assessment: A sustainability perspective. *International Journal of Production Research, 50*(19), 5474–5490.

Dou, Y., Zhu, Q., & Sarkis, J. (2014). Evaluating green supplier development programs with a grey-analytical network process-based methodology. *European Journal of Operational Research, 233*(2), 420–431.

Elkington, J. (1998). *Cannibals with forks: The triple bottom line of the 21st century business*. Stoney Creek, CT: New Society Publishers.

Elkington, J. (2004). Enter the triple bottom line. In A. Henriques & J. Richardson (Eds.), *The triple bottom line: Does it all add up* (pp. 1–16). London: Earthscan.

Foerstl, K., Reuter, C., Hartmann, E., & Blome, C. (2010). Managing supplier sustainability risks in dynamically changing environment—Sustainable supplier management in the chemical industry. *Journal of Purchasing and Supply Management, 16*(2), 118–130.

Gallardo-Vázquez, D., & Sanchez-Hernandez, M. I. (2014). Measuring corporate social responsibility for competitive success at a regional level. *Journal of Cleaner Production, 72,* 14–22.

Ghagde, A., Dani, S., & Kalawsky, R. (2012). Supply chain risk management: Present and future scope. *International Journal of Logistics Management, 23*(3), 313–339.

Giunipero, L. C., Hooker, R. E., & Denslow, D. (2012). Purchasing and supply management sustainability: Drivers and barriers. *Journal of Purchasing and Supply Management, 18*(4), 258–269.

Goncz, E., Skirke, U., Kleizen, H., & Barber, M. (2007). Increasing the rate of sustainable change: A call for redefinition of the concept and model for its implementation. *Journal of Cleaner Production, 15*(6), 525–537.

Greenfield, W. M. (2004). In the name of corporate social responsibility. *Business Horizons, 47,* 19–28.

GRI (2009). Transparency in the supply chain projects. News, Online. Retrieved February 20, 2015, from https://ww.lobalreporting.rg/esourcelibrary/lobal-ction-etwork-or-ransparency-n-he-upply-hain-rogram-verview.df.

Hallikas, J., Puumalainen, K., Vesterinen, T., & Virolainen, V.-M. (2005). Risk-based classification of supplier relationships. *Journal of Purchasing and Supply Management, 11*(2–3), 72–82.

Harwood, I., & Humby, S. (2008). Embedding corporate responsibility into supply: A snapshot of progress. *European Management Journal, 26*(3), 166–174.

Hofmann, H., Busse, C., Bode, C., & Henke, M. (2014). Sustainability-related supply chain risks: Conceptualization and management. *Business Strategy and the Environment, 23*(3), 160–172.

Holweg, M., Reichhart, A., & Hong, E. (2011). On risk and cost in global sourcing. *International Journal Production Economics, 131*(1), 333–341.

ISO/DIS 20400.2 (2016) Sustainable procurement—Guidance (draft manual).

Lee, M.-D. (2008). A review of the theories of corporate social responsibility: Its evolutionary path and the road ahead. *International Journal of Management Reviews, 10,* 53–73.

Lindgreen, A., Swaen, V. & Johnston, W. J. (2009). Corporate social responsibility: An empirical investigation of U.S. organizations. *Journal of Business Ethics*, *85*(Suppl. 2), 303–323.

Lindgreen, A., & Swaen, V. (2010). Corporate social responsibility. *International Journal of Management Reviews, 12*(1), 1–7.

Lonsdale, C. (1999). Effective managing vertical supply relationships: A risk management model for outsourcing. *Supply Chain Management: An international Journal*, *4*, 176–183.

Maignan, I., & Ralston, D. (2002). Corporate social responsibility in Europe and the U.S.: Insights from businesses' self-presentations. *Journal of International Business Studie, 33,* 497–514.

Manuj, I., & Mentzer, J. T. (2008). Global supply chain risk management. *Journal of Business Logistics, 29*(1), 133–155.

McWilliams, A., Siegel, D. S., & Wright, P. M. (2006). Corporate social responsibility: Strategic implications. *Journal of Management Studies*, *43*(1), 1–18.

Multaharju, S. (2016). *Managing sustainability-related risks in supply chains.* Acta Universitatis Lappeenrantaensis 725, Lappeenranta: Lappeenranta University of Technology Yliopistopaino.

Nidumolu, R., Prahalad, C. K., & Rangaswami, M. R. (2009). Why sustainability is now the key driver of innovation. *Harvard Business Review, 87*(9), 57–64.

Pearce, J. A., & Doh, J. P. (2005). High-impact collaborative social initiatives. *MIT Sloan Management Review, 46,* 30–39.

Schneider, L., & Wallenburg, C. M. (2012). Implementing sustainable sourcing—Does purchasing need to change? *Journal of Purchasing and Supply Management, 18*(4), 243–257.

Seuring, S., & Müller, M. (2008). From a literature review to a conceptual framework for sustainable supply chain management. *Journal of Cleaner Production, 16*(15), 1699–1710.

Sheldon, O. (1924). *The philosophy of management*. London: Isaac Pitman and Sons Ltd.

Sikdar, S. K. (2003). Sustainable development and sustainability metrics. *AIChE Journal, 49*(8), 1928–1932.

Simpson, D.F & Power, D. (2005) Use the supply relationship to develop lean and green suppliers. *Supply Chain Management: An International Journal*, *10*, 60–68.

World Commission on Environment and Development. (1987). *Our Common Future*. Oxford: Oxford University Press.

Zsidisin, G. (2003). A grounded definition of supply risk. *Journal of Purchasing and Supply Management, 9*(5–6), 217–224.

Chapter 17
The Relationship Between Firm Resilience to Supply Chain Disruptions and Firm Innovation

Mahour M. Parast, Sima Sabahi and Masoud Kamalahmadi

1 Introduction

In today's turbulent and uncertain environment, organizations are susceptible to supply chain disruptions (Ambulkar et al. 2015). Thus, a firm's resilience to supply chain disruptions is regarded as an important organizational capability that enables the firm to mitigate the effects of disruption and to remain competitive (Fiksel 2015; Ponomarov and Holcomb 2009). This requires organizations to develop capabilities and identify the best practices to become more responsive to supply chain disruptions (Blackhurst et al. 2011; Jüttner and Maklan 2011) and to become more resilient (Blackhurst et al. 2011; Craighead et al. 2007).

One of the capabilities contributing to a firm's resilience is innovation (Kamalahmadi and Parast 2016b). Reinmoeller and Van Baardwijk (2005) found that among the resilient enterprises they studied, the focus on innovation increased by 235% over 20 years. Golgeci and Ponomarov (2013) stated that resilience is a vital dimension of a firm's continuity, and innovativeness is one of the key enablers of resilience. In their empirical study on the impact of firm innovativeness on effective responses to supply chain disruption, they found that both firm innovativeness and innovation magnitude are positively associated with supply chain resilience. Akgün and Keskin (2014) studied 112 firms to examine the relationship between organizational resilience capacity, product innovation, and firm performance. Their results indicate

M. M. Parast (✉) · S. Sabahi
North Carolina A&T State University, Greensboro, NC, USA
e-mail: mahour@ncat.edu

S. Sabahi
e-mail: ssabahi@aggies.ncat.edu

M. Kamalahmadi
Indiana University, Bloomington, IN, USA
e-mail: maskamal@iu.edu

G. A. Zsidisin and M. Henke (eds.), *Revisiting Supply Chain Risk*, Springer Series in Supply Chain Management 7, https://doi.org/10.1007/978-3-030-03813-7_17

significant associations between resilience-capacity variables and a firm's product innovativeness, where product innovativeness mediates the relationship between a firm's resilience and its performance.

In an overview of the antecedents of organizational resilience, Kamalahmadi and Parast (2016b) identified firm innovation as an organizational capability that improves a firm's resilience to supply chain disruption. Although innovation has been viewed as a key component of a firm's long-term survival, the role of innovation in improving a firm's resilience has been overlooked (Kamalahmadi and Parast 2016b). Understanding how firm innovation and firm resilience are related is important because it helps organizations to invest in organizational capabilities that can improve both firm innovation and firm resilience. To achieve this goal, we examine the relationship between firm innovation and firm resilience through conducting a systematic literature review to determine the antecedents of firm innovation and firm resilience (Tranfield et al. 2003; Ghadge et al. 2012; Kamalahmadi and Parast 2016b).

In this chapter, we start in Sect. 2 with a review of the literature about the impact of innovation on firm resilience. Then in Sect. 3, we discuss the research process. The linkage between innovation and resilience is discussed in Sect. 4. Supply chain resilience and firm innovation are further discussed in Sects. 5 and 6, respectively. In Sect. 7, we discuss the organizational capabilities to improve both firm innovation and firm resilience, and we develop our propositions. In Sect. 8, we discuss future research, and in Sect. 9, we state our concluding remarks.

2 Literature Review: Firm Innovation and Firm Resilience

Three studies have examined the impact of firm innovation on improving organizational resilience. Reinmoeller and Van Baardwijk (2005) argue that the most resilient companies consistently pursue a dynamic balance of four innovation strategies: knowledge management, exploration, cooperation, and entrepreneurship. Their findings are based on analyses of companies with a record of outperforming their competitors between 1983 and 2002. They screened 231 Dutch companies listed on the Amsterdam Stock Exchange and found that the mix of innovation strategies used by the companies helped them improve their resilience over time.

Golgeci and Ponomarov (2013) studied the relationship between firm innovativeness, innovation magnitude, disruption severity, and supply chain resilience. Through administering a survey to senior-level managers of supply chains or operations in the US and European manufacturing companies, they found that both firm innovativeness and innovation magnitude positively affect supply chain resilience. Moreover, they found a positive relationship between innovation magnitude and disruption severity.

Finally, Akgün and Keskin (2014) studied how organizational capacity and a firm's product innovativeness and performance are related to each other. Using a survey method, they studied 112 firms and found that there is a strong relationship between a firm's resilience capacity and its product innovativeness capability. They also showed that product innovativeness mediates the relationship between a firm's resilience and its performance.

The above studies provide important theoretical and managerial implications about the relationship between innovation management and supply chain resilience. To further examine the relationship between firm innovation and supply chain resilience, we review the literature to identify organizational capabilities pertaining to both innovation management and supply chain resilience. We aim to provide a more nuanced explanation about the relationship between innovation and resilience through identifying key organizational practices that have direct impact on both innovation and resilience.

3 Research Process

In this study, we conducted a systematic literature review to identify the antecedents of supply chain resilience and innovation (Ghadge et al. 2012; Kamalahmadi and Parast 2016b; Tranfield et al. 2003). For supply chain resilience, we based our literature review on the study conducted by Kamalahmadi and Parast (2016b), which focused on organizational practices for supply chain resilience. To provide a more updated review of the literature, we used the databases *Google Scholar*, *Science Direct*, and *Emerald* to identify publications in the context of supply chain resilience.

We used keywords such as "resilient" and "resilience" to identify publications addressing supply chain resilience. We employed the same procedure to collect the related publications in the context of innovation. However, in addition to exploring high-quality journals in the field of operations management and operations research/management science and the aforementioned databases, we explored high-quality journals in the field of innovation management using the keyword "innovation". In order to identify high-quality journals, we used the widely accepted quality rating published by the Association of Business Schools (ABS), UK, as Academic Journal Guide (AJG) 2015. Our research process found 56 publications related to the antecedents of firm resilience and firm innovation; these publications will be discussed in the upcoming sections.

In the next sections, we first discuss theoretical arguments regarding the relationship between firm innovation and firm resilience. We then review the existing body of knowledge in supply chain resilience and innovation management to identify organizational capabilities that lead to enhanced resilience and improved organizational innovation. These identified capabilities provide the basis for understanding the relationship between firm innovation and firm resilience, which will show how organizations can improve both innovation and resilience capabilities through investment in certain organizational capabilities.

4 The Linkage Between Innovation and Resilience: A Dynamic Capability View

The relationship between firm innovation and supply chain disruption management can be explained through the principles and premises of the dynamic capabilities theory of the firm (Teece 2007). The dynamic capability of a firm is an organizational capability to recreate resources and capabilities to resolve problems, scan for opportunities, and mitigate the possible adverse effects of disruption, in order to remain relevant and competitive in a turbulent environment (Barreto 2010; Di Stefano et al. 2010). As an extension of the resource-based view of the firm, dynamic capabilities theory has a specific focus on innovation and creating value (Katkalo et al. 2010). Because value creation and development of new capabilities are the results of innovative activities of a firm (Ellonen et al. 2009; Teece 2007), dynamic capabilities theory is an appropriate theoretical lens that relates firm innovation to firm resilience and organizational performance in turbulent environments. It is the innovation capability of a firm that enables it to respond to environmental change, develop solutions to emerging problems, and take necessary actions.

The linkage between innovation management and supply chain disruption risk management can be examined through understanding their relationship to change. Both innovation management and risk management are concerned with the ability of an organization to develop capabilities to be adaptive and to respond to change (Walker et al. 2006). While risk management entails development of capabilities to mitigate the negative impact of unfavorable outcomes, innovation management is concerned with activities that lead to desired (i.e., positive) outcomes. Risk management and innovation management are both concerned with an organizational response to change; however, while an organization deliberately embarks on innovation investment to develop new products and services, risk management programs are institutionalized to respond to undesirable shocks and threats. Thus, they both are concerned with organizational capability, but with different emphasis.

There are also differences between risk management and innovation management with respect to how organizations view them. Innovation management is seen as a proactive activity that aims to enhance a firm's competitive position, so innovation is usually associated with growth (Cho and Pucik 2005; Crossan and Apaydin 2010; Garcia and Calantone 2002). Risk management is usually regarded as a practice to maintain and sustain the current organizational structures, norms, and practices and to ensure that the firm has plans in place to continue its normal operations in the event of disruptions, so risk management is seen as more of a reactive firm behavior (Bode et al. 2011). A core capability common to both resilient and innovative organizations is their ability to anticipate changes in the environment and their ability to proactively learn. At the conceptual level, both risk management and innovation management are concerned with change, but they deal with it in different ways. Thus, it is expected that organizations would be able to improve both their innovation and their resilience through investment in certain organizational capabilities that are antecedents of both innovation and resilience. In the following sections, we review the literature to identify the antecedents of firm innovation and firm resilience, to look for commonality between them.

5 Supply Chain Resilience

Kamalahmadi and Parast (2016b) defined supply chain resilience as “the adaptive capability of a supply chain to reduce the probability of facing sudden disturbances, resist the spread of disturbances by maintaining control over structures and functions, and recover and respond by immediate and effective reactive plans to transcend the disturbance and restore the supply chain to a robust state of operations” (p. 121). While different definitions for supply chain resilience are introduced in the literature, they all refer to it as the capability of a firm and its supply chain to mitigate the adverse effects of supply chain disruptions. Thus, to better understand the linkage between innovation and resilience, we need to first identify the organizational capabilities that enhance firm responsiveness to supply chain disruptions. These capabilities are discussed in the following section.

5.1 Antecedents of Supply Chain Resilience

Kamalahmadi and Parast (2016b) conducted a comprehensive review of the antecedents of supply chain resilience. In this section, we review these capabilities and identify those most frequently addressed by authors. These capabilities are summarized in Table 1.

Flexibility. Flexibility is defined as the ability to take different positions to better react to unusual situations and swiftly adjust to significant changes in the supply chain (Lee and Cameron 2004). Having flexible transportation systems, flexible production facilities, a flexible supply base, flexible capacity, and flexible labor arrangements are examples of the ways that flexibility can strengthen resilience (Colicchia et al. 2010; Tang and Tomlin 2008; Tang 2006; Tomlin 2006; Yang and Yang 2010).

Redundancy. Another way to improve resiliency is through creating redundancies across a supply chain. Having multiple suppliers, safety stock, overcapacity, and backup suppliers are examples of redundancies in supply chains (Knemeyer et al. 2009; Sheffi 2005; Sodhi and Lee 2007; Tang 2006; Tomlin 2006).

Collaboration. Nishat Faisal et al. (2006) interpret collaboration as the “glue that holds supply chain organizations in a crisis together”. Cooperation diminishes uncertainty by distributing risk (Reinmoeller and Van Baardwijk 2005). An empirical study by Wieland and Marcus Wallenburg (2013) on the influences of relational competencies (communication, cooperation, and integration) on supply chain resilience revealed that communicative and cooperative relationships have a positive impact on resilience. A survey conducted by Soni et al. (2014) found that collaboration is ranked second among 14 enablers of supply chain resilience.

Table 1 Antecedents of firm resilience

Capability	Related literature
Redundancy	Azadeh et al. (2014), Knemeyer et al. (2009), Sheffi (2005), Sodhi and Lee (2007), Tang (2006), Tomlin (2006)
Flexibility	Lee and Cameron (2004), Colicchia et al. (2010), Tang and Tomlin (2008), Tang (2006), Tomlin (2006), Yang and Yang (2010)
Collaboration	Christopher and Peck (2004), Pettit et al. (2010), Faisal et al. (2006), Reinmoeller and Van Baardwijk (2005), Wieland and Marcus Wallenburg (2013), Soni et al. (2014), Borekci et al. (2015), Scholten and Schilder (2015)
Trust	Nishat Faisal et al. (2007), Raj Sinha et al. (2004), Ponomarov and Holcomb (2009), Wicher and Lenort (2012), Soni et al. (2014)
Information sharing	Scholten and Schilder (2015), Mandal (2012), Wicher and Lenort (2012), Melnyk (2014), Priya Datta et al. (2007), Soni et al. (2014), Blackhurst et al. (2011)
Agility	Wieland and Marcus Wallenburg (2013), Cabral et al. (2012), Soni et al. (2014)
Visibility	Soni et al. (2014), Wieland and Marcus Wallenburg (2013), Azadeh et al. (2014), Brandon-Jones et al. (2014), Johnson et al. (2013), Ponis and Koronis (2012), Wilding (2013)
Velocity	Prater et al. (2001), Wieland and Marcus Wallenburg (2013), Scholten et al. (2014), Carvalho et al. (2012), Wicher and Lenort (2012)
Supply chain risk management culture	Christopher and Peck (2004), Moore and Manring (2009), Sheffi (2005), Ates and Bititci (2011), Christopher et al. (2011), Mandal (2012), Soni et al. (2014)
Leadership	Christopher and Peck (2004), Wilding (2013), Demmer et al. (2011), Rice and Caniato (2003), Blackhurst et al. (2011)

Trust. According to Faisal et al. (2007), trust makes cooperation and collaboration easier, both within the organization and across partners in the supply chain. Ponomarov and Holcomb (2009) analyzed the mutual trusting behaviors of buyer—supplier resilience and found that a greater degree of mutual trusting behaviors can support greater relational resilience in buyer–supplier relationships. In their study, a trusted network is required for the design of a cooperative relationship, and consequently, a trusted network increases the resilience of supply chains. Respondents to the survey conducted by Soni et al. (2014) ranked trust as the seventh most important out of 14 enablers of supply chain resilience.

Information sharing. According to Christopher and Peck (2004), the key element for collaborative working and risk reduction should involve the building of a resilient supply chain where there is the exchange of information among members of the supply chain. Mandal (2012) stated that collaboration can only take place when each member receives relevant information efficiently and effectively. Investment in sharing information and monitoring performance can help identify potential problems in a supply chain (Melnyk 2014). In a multi-case analysis, six out of seven enterprises highlighted the need to have predefined communication protocols in order to minimize the effects of disruptions through effective information sharing (Blackhurst et al. 2011).

Agility. Agility is defined as "the ability of a supply chain to rapidly respond to change by adapting its initial stable configuration" (Wieland and Marcus Wallenburg 2012, p. 890). Wieland and Marcus Wallenburg (2013) stated that supply chain resilience has two aspects: (1) a proactive dimension, which is concerned with robustness; and (2) a reactive dimension, which deals with agility. Two elements of agility suggested by Christopher and Peck (2004) are visibility and velocity (Azadeh et al. 2014; Faisal et al. 2006; Scholten et al. 2014; Wieland and Marcus Wallenburg 2013).

Spiegler et al. (2012) stated that supply chains will encounter extreme changes in their resilience performance when lead time changes. Reductions in lead time for production and transportation are emphasized by Carvalho et al. (2012) as practices that enhance agility and resilience.

Supply chain risk management culture. According to Christopher and Peck (2004), organizations need to incorporate a culture for supply chain risk management in order to construct a resilient organization. Organizational behavior and characteristics are major factors in the evolution toward resilient and sustainable enterprises (Moore and Manring 2009). Sheffi (2005) asserted that the key difference between successful and unsuccessful response to disruptions is organizational culture.

Ates and Bititci (2011) examined the role of culture and change management in resilience in small and medium-sized enterprises. They found that incorporating, developing, and implementing change capabilities are significant in making progress toward sustainability and resilience in organizations. The results of an empirical study by Mandal (2012) show that a culture of risk management must be embedded in the focal firm and across its supply chain members. Soni et al. (2014) described risk management culture as one of the major drivers of resilience.

Leadership. Christopher and Peck (2004) noted that within the process of cultural change at the organizational level, nothing is achievable without support and commitment from the leadership. Wilding (2013) stated that introducing a risk management culture forces the leadership to review company policies and practices and to determine their impact on the risk profile of the supply chain. An empirical study by Blackhurst et al. (2011) found that education and training of supply chain employees were identified by six of the seven firms as a main component in enhancing their firm's capabilities in supply chain resilience.

Now, we turn our focus to firm innovation and to better understand the importance of innovation in firm and supply chain level and identify the antecedents enhancing innovation performance.

6 Firm Innovation

In order to respond to swift changes in products, services, customer's demands, and problems, firms need to have innovation capability (Christopher 2005; Kim et al.

2015). Innovation generally occurs in processes, technologies, services, strategies, and organizational structures (Rogers 2003). Innovation pertains to new applications of knowledge, ideas, methods, and skills that can create distinctive capabilities and influence an organization's competitiveness (Andersson et al. 2008; Fagerberg and Verspagen 2009). In the context of supply chains, innovation focuses on addressing the demands of the marketplace, which can consequently increase value propositions for customers (Flint et al. 2008). Panayides et al. (2005, pp. 192–193) said "As supply chain parties become more innovative in terms of adopting new processes, operational routines and investing in new technological systems, supply chain effectiveness in terms of ability to fulfill what was promised, meet standards and solve problems will improve."

Empirical studies on innovation have investigated five types of innovation: incremental product, incremental process, radical product, radical process, and administrative (Di Benedetto et al. 2008; Herrmann et al. 2007; Salavou and Lioukas 2003). Innovation can be divided into incremental innovation and radical innovation when considering the following characteristics of innovation: the level of change (minor vs. major), a target customer or market (existing vs. new), and the level of risk (low vs. high). Another common categorization of innovation is in terms of technological vs. administrative, where technological innovation encompasses both product and process innovation (Kim et al. 2012). A comprehensive comparison of radical, incremental, and administrative innovation is shown in Table 2. A brief discussion of the different types of innovation follows the table.

Product, process, and administrative innovation. Product innovation is defined as changes at the end of providing products or services, while process innovation refers to changes in the method of producing products or services (Propris 2002). Process innovation is considered as changes in the way that a firm produces products or services (Koberg et al. 2003). Process innovation changes the sequences and nature of the production process to enhance the productivity and efficiency of production activities (Garcia and Calantone 2002; Propris 2002). Administrative innovation is defined as the application of new ideas to improve organizational structures and systems or to improve processes involving the social structure of an organization (Weerawardena 2003). Administrative innovation is often prompted by internal needs for structuring and coordination (Daft 1978; Gaertner et al. 1984).

Incremental versus radical innovation. Incremental innovation pertains to slight changes of existing technologies in terms of design, function, price, quantity, and features to meet the needs of existing customers (Garcia and Calantone 2002; Propris 2002). Radical innovation refers to the adoption of new technologies to create a demand not yet realized by customers and markets (Jansen et al. 2006). Incremental innovation emphasizes refining, broadening, enhancing, and exploiting current knowledge, skills, and technical trajectory (Gatignon et al. 2002), while radical innovation focuses on market pull or technology push strategies (Li et al. 2008). Incremental innovation is associated with a lower level of risk and modest potential benefits (Koberg et al. 2003); radical innovation is associated with a higher level of risk and great uncertainty (Moguilnaia et al. 2005).

Table 2 Comparison of technological and administrative innovation (Kim et al. 2012)

Dimension	Technological innovation		Administrative innovation
	Radical innovation	Incremental innovation	
Objective	Create new markets with new customers by responding to a previously unrecognized demand, replacing old technologies, or disrupting a current technology trajectory	Meet needs of existing customers by refining, broadening, or combining a current technical trajectory, knowledge, and skills	Increase the efficiency and the effectiveness of managerial systems and processes by obtaining new resources or adopting new programs
Subject of innovation	Radical product innovation: products or services. Radical process innovation: processes	Incremental product innovation: products or services. Incremental process innovation: processes	Structures, policies, systems, and processes of management and organization
Level of change	Major changes of technological directions, approaches, or linkage among core components	Minor changes of existing components, design, price, function, quantity, or time	Both major and minor changes
Approach	Mainly a bottom-up approach initiated by lower-level technicians and R&D workers	Mainly a bottom-up approach conducted by lower-level technicians and R&D workers	Mainly a top-down approach initiated by upper-level managers or administrators
Level of risk	A high level of risk due to a high degree of complexity and technical/market uncertainties	A low level of risk due to a greater level of certainty with known information	High risk and low risk
Output	Occur rarely but create entirely new product categories; identify unrecognized demands or methods; result in technological and marketing discontinuities; restructure marketplace economics	Occur often and enrich the depth of technology innovation; improve certain dimensions of products or processes; expand brands and product categories; develop existing competencies	Enhance organizational structures, administrative systems, and processes; add value directly for a firm or indirectly for its customers
Protection of output	Mainly protected by intellectual property law, such as patent; diffused under the technology transfer contract	Mainly protected by intellectual property law, such as patent; diffused under the technology transfer contract	Mainly not protected by intellectual property law; diffused by specialized agents (e.g., consulting firms)

6.1 Antecedents of Firm Innovation

Since our purpose is to explore the relationship between a firm's innovation capability and the firm's supply chain resilience, we identify innovation antecedents that show a significant relationship to firm resilience.

Leadership. A study by Vaccaro et al. (2012) showed that leadership behavior is a key driver for innovation. Also, the effect of senior leadership on employee creativity and team innovation was investigated by Yoshida et al. (2014). Dunne et al. (2016) analyzed responses collected from entrepreneurs and found that leadership style, negotiation style, and organizational efficacy each positively affect new product innovation.

Collaboration. As innovation expands to all firm personnel and departments, it should be thought of as a collaborative application (Ar and Baki 2011). In fact, innovative capabilities depend on communication between individuals, groups, organizations, and subsystems, because such communications intensify knowledge and learning (Ar and Baki 2011). Krolikowski and Yuan (2017) provide an empirical investigation of the impact of customer–supplier relationships on firm innovation. Their study indicated that a concentrated customer base promotes suppliers to invest more in research and development (R&D) and become more innovative. Fossas-Olalla et al. (2015) show that firms that collaborate technologically with suppliers have a greater potential for product innovation. Un and Asakawa (2015) explained how R&D collaborations affect process innovation. Their results indicate that R&D collaborations with suppliers and universities appear to have a positive impact on process innovation. Yao et al. (2013) found that in a supply chain, collaborative forecasting and collaborative replenishment exhibit distinct learning curves. Their finding is additional support for the positive impact of collaboration on innovation, if we accept that firms that learn more are more innovative.

Knowledge sharing. Firms need to share some of their own knowledge in order to have access to external knowledge that may expand or improve their innovation activities (Ritala et al. 2015). Ritala et al. (2015) examined the quandary of external knowledge sharing and knowledge leakage. They found out that external knowledge sharing increases the relative innovation performance of the firm. However, accidental and intentional knowledge leakage negatively moderate this relationship. Moreover, according to Bellamy et al. (2014), improved knowledge and information flows arising from supply network accessibility positively affect a firm's innovation output.

R&D strategy. R&D is considered as the key prerequisite driving technological change, which is closely linked with innovation (Avermaete et al. 2004). To create or adopt new products or processes in the marketplace and to be innovative, firms need to emphasize and invest in R&D (Gu and Tang 2004). Thus, the amount of R&D expenditures, resources, and personnel is usually used to measure the input to the innovation process. Ar and Baki (2011) demonstrated that R&D strategy has a direct effect on the level of product innovation, while it has an indirect effect on process innovation.

Capability for creativity. Creativity refers to the ability to develop new ideas, products, or services based on perceived patterns and relationships (Scozzi et al. 2005). In terms of innovation, the production of novel and useful ideas is often an important part of the innovation process (Mathisen et al. 2004). Carayannis and Gonzalez (2003) stated that creativity (mostly at the individual level) is a requisite factor enabling innovation (mostly at the organizational level). Furthermore, Gumusluoglu and Ilsev (2009) state that creativity at the individual level, through new idea generation and implementation, is likely to cause the development of innovative products. As a result, it can be said that creativity is a driving factor in enhancing innovation (Ar and Baki 2011).

7 Organizational Capabilities to Improve Both Firm Innovation and Firm Resilience

Innovation is a key element for an enterprise's long-term survival and growth, and it plays a vital role in how a firm adapts to changes in the environment (Santos-Vijande and Álvarez-González 2007). Firms with greater innovativeness will be more successful in responding to customers' needs and in developing new capabilities that allow the firm to achieve better performance or superior profitability (Calantone et al. 2002; Sadikoglu and Zehir 2010). On the other hand, as discussed earlier, supply chain risk management not only helps organizations to develop their resilience to disruption, but also contributes to firm performance (Liu et al. 2017). Thus, we have two perspectives, innovation and resilience, that improve firm performance in two different ways. If innovation and resilience share some antecedent capabilities, a firm could strengthen those capabilities to enhance both resilience and innovation. Table 3 presents capabilities that are shared between innovation and resilience. We develop our propositions regarding the relationship between firm innovation and firm resilience as follows.

Collaboration. In an organization, cooperation between departments is a driver of innovation (Brouwer and Kleinknecht 1996; Hyvärinen 1990), because innovation capability depends on the interaction between individuals, groups, organizations, and subsystems (Ilker Murat and Birdogan 2011). It has also been shown that cross-functional integration in the form of collaboration significantly affects innovation performance (Frishammar and Åke Hörte 2005). Collaboration with suppliers, clients, and research organizations has a positive impact on innovation (Nieto and Santamaría 2007; Ritala et al. 2015). As a result, firms that want to become more innovative need to strengthen their collaboration capability and consider collaboration as a key driver, because the success of firm innovation relies on the extent to which a firm exhibits collaborative behavior. Apart from the significant effect of collaboration on innovation, several studies have discussed the impact of collaboration on improving firm resilience (Pettit et al. 2010; Wieland et al. 2013; Borekci et al. 2015). In fact, collaboration leads to mitigating uncertainty and increasing readiness

Table 3 Capabilities common to innovation and resilience

Capability	Innovation	Resilience
Collaboration	Ar and Baki (2011), Krolikowski and Yuan (2017), Fossas-Olalla et al. (2015), Un and Asakawa (2015), Yao et al. (2013)	Christopher and Peck (2004), Pettit et al. (2010), Nishat Faisal et al. (2006), Reinmoeller and Van Baardwijk (2005), Wieland and Marcus Wallenburg (2013), Soni et al. (2014), Borekci et al. (2015), Scholten and Schilder (2015)
Information Sharing	Ritala et al. (2015), Bellamy et al. (2014)	Scholten and Schilder (2015), Mandal (2012), Melnyk (2014), Priya Datta et al. (2007), Soni et al. (2014), Blackhurst et al. (2011)
Leadership	Ar and Baki (2011), Vaccaro et al. (2012), Yoshida et al. (2014), Dunne et al. (2016), Ryan and Tipu (2013), Montes et al. (2005)	Christopher and Peck (2004), Wilding (2013), Demmer et al. (2011), Rice and Caniato (2003), Blackhurst et al. (2011)

for unpredicted events (Christopher and Peck 2004). As a result, in a collaborative environment, firms are more resilient to disruptions (Christopher and Peck 2004; Reinmoeller and Van Baardwijk 2005; Soni et al. 2014; Wieland and Marcus Wallenburg 2013). Thus, we propose the following:

Proposition 1 *Firms with an innovative environment are more resilient to disruption because they have more collaboration.*

Information Sharing. Knowledge-sharing practices in firms are suggested as contributing to competitive advantage (Wang and Wang 2012). A firm's ability to transform and exploit knowledge may determine its level of innovation (Wang and Wang 2012). Bellamy et al. (2014) and Ritala et al. (2015) have shown the positive effect of knowledge sharing on innovation. In fact, knowledge sharing offers a great opportunity to explore and examine the possible (market) value and opportunities for that knowledge (Chesbrough 2006), which are considered as significant factors for a firm's innovation (Ritala et al. 2015). For example, a firm can demonstrate the potential value of the knowledge by sharing it with the external partners and even the competitors (Husted and Michailova 2010). Thus, knowledge-sharing capability increases the firm's attractiveness as a potential partner in inter-firm innovation projects. In addition, external knowledge sharing improves the firm strategic network position (Ritala et al. 2015), as a result of expediting the path to potential value and promising outcomes (Clarysse et al. 1996). This increases a firm's opportunity to broaden the range of innovation capabilities and processes (Brusoni et al. 2001). Firms can improve their performance in terms of innovation as they rely on shared knowledge and competencies (Demmer et al. 2011; Gupta and Polonsky 2014).

Thus, knowledge-sharing mechanisms have a profound impact on both improving firm innovation and firm resilience. Current thinking in supply chain management views information sharing as one of the key elements for successfully managing and coordinating supply chains (Ganesh et al. 2014). According to Christopher and Peck (2004), the key priority for risk reduction should be the creation of a supply chain community where there is an exchange of information among members of the supply chain. According to Soni et al. (2014), internal and external knowledge sharing are considered as two antecedents of resilience in large enterprises. Therefore, we propose the following:

Proposition 2 *Innovative firms are more resilient to disruption because they have more information-sharing capability.*

Leadership. A leader supports teams and individuals as they turn their creative efforts into innovations (leader as facilitator); a leader also manages the organization's goals and activities aimed at innovation (leader as manager) (Denti and Hemlin 2012). For example, Dunne et al. (2016) found that leadership style, organizational efficacy, and negotiation style are three measures of leadership that have a positive effect on a firm's innovativeness. In fact, top managers have a crucial role in boosting innovation because innovation is a complex system (Ilker Murat and Birdogan 2011). In addition, for implementing innovation, firms need to consider the leader's view about innovation as a necessary element (Senge 1990). Since leaders shape employee's innovative behavior through their deliberate actions aiming to stimulate idea generation (De Jong and Den Hartog 2007), there must be a culture that both supports and rewards employee's innovative ideas (Wan et al. 2005). Such an innovation-supportive culture is created by leaders. In addition to supporting innovative ideas, Carayannis and Gonzalez (2003) showed that supportive management is regarded as one of the innovation catalysts, because a supportive manager is willing to take risks and stimulate fresh thinking.

From the risk management perspective, several authors have shown the influential effect of supportive leadership on a firm's resilience (Blackhurst et al. 2011; Christopher and Peck 2004; Demmer et al. 2011). In every case of culture change at an organizational level, without a supportive leadership, nothing is possible (Christopher and Peck 2004). Instilling a risk management culture requires the leadership to review company policies and practices, to determine their impact on the risk profile of the supply chain (Wilding 2013). Regarding the positive impact of supportive leadership on firm innovation and resilience, we propose the following:

Proposition 3 *More innovative firms are more resilient to disruption because they need to have more supportive leadership capability.*

8 Future Research

There are several avenues for exploring the relationship between firm innovation, firm resilience, and firm performance. First, there might be other innovation capabilities that we failed to notice in this study. Consequently, the first future direction could be a comprehensive review of innovation from different perspectives, analyzing their relationship with supply chain resilience. Second, development of a conceptual and theoretical model to relate innovation, resilience, and firm performance would be instrumental in theory development. Third, in this research, the impact of innovation type on resilience and innovation capabilities was not investigated. For example, it is not known whether firms involved in process innovation are more resilient in responding to supply chain disruption than firms that are not involved in process innovation. In addition, an examination of the relative importance of the level of innovation change (radical vs. incremental) on improving firm resilience would be an interesting research area. Therefore, another future direction is to explore the impact of innovation type on both innovation and resilience. Finally, capabilities discussed in this study were examined regardless of a firm's size and industrial segment. Both size and industrial segments play important roles in identifying key antecedents, so future research is needed to explore key antecedents considering a firm's size and industrial segment.

9 Conclusion

In this chapter, we investigated the relationship between supply chain resilience and innovation. Through reviewing two streams of research (innovation and resilience), we were able to identify key practices that improve both organizational innovation and resilience. We discussed how leadership, information sharing, and collaboration, which are antecedents of both resilience and innovation, contribute to making innovative firms more resilient. Organizations would be able to improve their resilience to supply chain disruptions through emphasizing their innovation capabilities.

Acknowledgements This research is based upon work supported by the National Science Foundation (NSF) under Grant number 123887 (Research Initiation Award: Understanding Risks and Disruptions in Supply Chains and their Effect on Firm and Supply Chain Performance).

References

Ajgün, A. E., & Keskin, H. (2014). Organisational resilience capacity and firm product innovativeness and performance. *International Journal of Production Research, 52*(23), 6918–6937.

Ambulkar, S., Blackhurst, J., & Grawe, S. (2015). Firm's resilience to supply chain disruptions: Scale development and empirical examination. *Journal of Operations Management, 33,* 111–122.

Andersson, M., Lindgren, R., & Henfridsson, O. (2008). Architectural knowledge in inter-organizational IT innovation. *The Journal of Strategic Information Systems, 17*(1), 19–38.

Ar, I. M., & Baki, B. (2011). Antecedents and performance impacts of product versus process innovation: Empirical evidence from SMEs located in Turkish science and technology parks. *European Journal of Innovation Management, 14*(2), 172–206.

Ates, A., & Bititci, U. (2011). Change process: A key enabler for building resilient SMEs. *International Journal of Production Research, 49*(18), 5601–5618.

Avermaete, T., Viaene, J., Morgan, E. J., Pitts, E., Crawford, N., & Mahon, D. (2004). Determinants of product and process innovation in small food manufacturing firms. *Trends in Food Science & Technology, 15*(10), 474–483.

Azadeh, A., Atrchin, N., Salehi, V., & Shojaei, H. (2014). Modelling and improvement of supply chain with imprecise transportation delays and resilience factors. *International Journal of Logistics Research and Applications, 17*(4), 269–282.

Barreto, I. (2010). Dynamic capabilities: A review of past research and an agenda for the future. *Journal of Management, 36*(1), 256–280.

Bellamy, M. A., Ghosh, S., & Hora, M. (2014). The influence of supply network structure on firm innovation. *Journal of Operations Management, 32*(6), 357–373.

Blackhurst, J., Dunn, K. S., & Craighead, C. W. (2011). An empirically derived framework of global supply resiliency. *Journal of business logistics, 32*(4), 374–391.

Bode, C., Wagner, S. M., Petersen, K. J., & Ellram, L. M. (2011). Understanding responses to supply chain disruptions: Insights from information processing and resource dependence perspectives. *Academy of Management Journal, 54*(4), 833–856.

Brandon-Jones, E., Squire, B., Autry, C. W., & Petersen, K. J. (2014). A contingent resource-based perspective of supply chain resilience and robustness. *Journal of Supply Chain Management, 50*(3), 55–73.

Brouwer, E., & Kleinknecht, A. (1996). Firm size, small business presence and sales of innovative products: A micro-econometric analysis. *Small Business Economics, 8*(3), 189–201.

Brusoni, S., Prencipe, A., & Pavitt, K. (2001). Knowledge specialization, organizational coupling, and the boundaries of the firm: Why do firms know more than they make? *Administrative Science Quarterly, 46*(4), 597–621.

Cabral, I., Grilo, A., & Cruz-Machado, V. (2012). A decision-making model for lean, agile, resilient and green supply chain management. *International Journal of Production Research, 50*(17), 4830–4845.

Calantone, R. J., Cavusgil, S. T., & Zhao, Y. (2002). Learning orientation, firm innovation capability, and firm performance. *Industrial Marketing Management, 31*(6), 515–524.

Carayannis, E. G., & Gonzalez, E. (2003). Creativity and innovation = competitiveness? When, how, and why. In L. V. Shavinina (Ed.), *The international handbook on innovation (part VIII)* (pp. 587–606). Amsterdam: Elsevier.

Carvalho, H., Azevedo, S. G., & Cruz-Machado, V. (2012). Agile and resilient approaches to supply chain management: Influence on performance and competitiveness. *Logistics Research, 4*(1–2), 49–62.

Chesbrough, H. W. (2006). *Open innovation: The new imperative for creating and profiting from technology*. Boston: Harvard Business Press.

Cho, H. J., & Pucik, V. (2005). Relationship between innovativeness, quality, growth, profitability, and market value. *Strategic Management Journal, 26*(6), 555–575.

Christopher, M. (2005). *Logistics & supply chain management: Creating value-adding networks (financial times series)*. Boston: Harvard Business School Press.

Christopher, M., Mena, C., Khan, O., & Yurt, O. (2011). Approaches to managing global sourcing risk. *Supply Chain Management: An International Journal, 16*(2), 67–81.

Christopher, M., & Peck, H. (2004). Building the resilient supply chain. *The International Journal of Logistics Management, 15*(2), 1–14.

Clarysse, B., Debackere, K., & Rappa, M. A. (1996). Modeling the persistence of organizations in an emerging field: The case of hepatitis C. *Research Policy, 25*(5), 671–687.

Colicchia, C., Dallari, F., & Melacini, M. (2010). Increasing supply chain resilience in a global sourcing context. *Production Planning & Control, 21*(7), 680–694.

Craighead, C. W., Blackhurst, J., Rungtusanatham, M. J., & Handfield, R. B. (2007). The severity of supply chain disruptions: Design characteristics and mitigation capabilities. *Decision Sciences, 38*(1), 131–156.

Crossan, M. M., & Apaydin, M. (2010). A multi-dimensional framework of organizational innovation: A systematic review of the literature. *Journal of Management Studies, 47*(6), 1154–1191.

Daft, R. L. (1978). A dual-core model of organizational innovation. *Academy of Management Journal, 21*(2), 193–210.

De Jong, J. P., & Den Hartog, D. N. (2007). How leaders influence employees' innovative behaviour. *European Journal of Innovation Management, 10*(1), 41–64.

Demmer, W. A., Vickery, S. K., & Calantone, R. (2011). Engendering resilience in small-and medium-sized enterprises (SMEs): A case study of Demmer Corporation. *International Journal of Production Research, 49*(18), 5395–5413.

Denti, L., & Hemlin, S. (2012). Leadership and innovation in organizations: A systematic review of factors that mediate or moderate the relationship. *International Journal of Innovation Management, 16*(03), 1240007.

Di Benedetto, C. A., DeSarbo, W. S., & Song, M. (2008). Strategic capabilities and radical innovation: An empirical study in three countries. *IEEE Transactions on Engineering Management, 55*(3), 420–433.

Di Stefano, G., Peteraf, M., & Verona, G. (2010). Dynamic capabilities deconstructed‡: A bibliographic investigation into the origins, development, and future directions of the research domain. *Industrial and Corporate Change, 19*(4), 1187–1204.

Dunne, T. C., Aaron, J. R., McDowell, W. C., Urban, D. J., & Geho, P. R. (2016). The impact of leadership on small business innovativeness. *Journal of Business Research, 69*(11), 4876–4881.

Ellonen, H.-K., Wikström, P., & Jantunen, A. (2009). Linking dynamic-capability portfolios and innovation outcomes. *Technovation, 29*(11), 753–762.

Fagerberg, J., & Verspagen, B. (2009). Innovation studies—the emerging structure of a new scientific field. *Research Policy, 38*(2), 218–233.

Fiksel, J. (2015). *From risk to resilience Resilient by Design* (pp. 19–34). Washington: Springer.

Flint, D. J., Larsson, E., & Gammelgaard, B. (2008). Exploring processes for customer value insights, supply chain learning and innovation: An international study. *Journal of Business Logistics, 29*(1), 257–281.

Fossas-Olalla, M., Minguela-Rata, B., López-Sánchez, J.-I., & Fernández-Menéndez, J. (2015). Product innovation: When should suppliers begin to collaborate? *Journal of Business Research, 68*(7), 1404–1406.

Frishammar, J., & Åke Hörte, S. (2005). Managing external information in manufacturing firms: The impact on innovation performance. *Journal of Product Innovation Management, 22*(3), 251–266.

Gaertner, G. H., Gaertner, K. N., & Akinnusi, D. M. (1984). Environment, strategy, and the implementation of administrative change: The case of civil service reform. *Academy of Management Journal, 27*(3), 525–543.

Ganesh, M., Raghunathan, S., & Rajendran, C. (2014). The value of information sharing in a multi-product, multi-level supply chain: Impact of product substitution, demand correlation, and partial information sharing. *Decision Support Systems, 58,* 79–94.

Garcia, R., & Calantone, R. (2002). A critical look at technological innovation typology and innovativeness terminology: A literature review. *Journal of Product Innovation Management, 19*(2), 110–132.

Gatignon, H., Tushman, M. L., Smith, W., & Anderson, P. (2002). A structural approach to assessing innovation: Construct development of innovation locus, type, and characteristics. *Management Science, 48*(9), 1103–1122.

Ghadge, A., Dani, S., & Kalawsky, R. (2012). Supply chain risk management: Present and future scope. *The International Journal of Logistics Management, 23*(3), 313–339.

Golgeci, I. & Y. Ponomarov, S. (2013). Does firm innovativeness enable effective responses to supply chain disruptions? An empirical study. *Supply Chain Management: An International Journal, 18*(6), 604–617.

Gu*, W. & Tang, J. (2004). Link between innovation and productivity in Canadian manufacturing industries. *Economics of Innovation and New Technology, 13*(7), 671–686.

Gumusluoglu, L., & Ilsev, A. (2009). Transformational leadership, creativity, and organizational innovation. *Journal of Business Research, 62*(4), 461–473.

Gupta, S., & Polonsky, M. (2014). Inter-firm learning and knowledge-sharing in multinational networks: An outsourced organization's perspective. *Journal of Business Research, 67*(4), 615–622.

Herrmann, A., Gassmann, O., & Eisert, U. (2007). An empirical study of the antecedents for radical product innovations and capabilities for transformation. *Journal of Engineering and Technology Management, 24*(1), 92–120.

Husted, K., & Michailova, S. (2010). Dual allegiance and knowledge sharing in inter-firm R&D collaborations. *Organizational Dynamics, 39*(1), 37–47.

Hyvärinen, L. (1990). Innovativeness and its indicators in small-and medium-sized industrial enterprises. *International Small Business Journal, 9*(1), 64–79.

Ilker Murat, A., & Birdogan, B. (2011). Antecedents and performance impacts of product versus process innovation: Empirical evidence from SMEs located in Turkish science and technology parks. *European Journal of Innovation Management, 14*(2), 172–206.

Jansen, J. J., Van Den Bosch, F. A., & Volberda, H. W. (2006). Exploratory innovation, exploitative innovation, and performance: Effects of organizational antecedents and environmental moderators. *Management Science, 52*(11), 1661–1674.

Johnson, N., Elliott, D., & Drake, P. (2013). Exploring the role of social capital in facilitating supply chain resilience. *Supply Chain Management: An International Journal, 18*(3), 324–336.

Jüttner, U., & Maklan, S. (2011). Supply chain resilience in the global financial crisis: An empirical study. *Supply Chain Management: An International Journal, 16*(4), 246–259.

Kamalahmadi, M., & Parast, M. M. (2016a). Developing a resilient supply chain through supplier flexibility and reliability assessment. *International Journal of Production Research, 54*(1), 302–321.

Kamalahmadi, M., & Parast, M. M. (2016b). A review of the literature on the principles of enterprise and supply chain resilience: Major findings and directions for future research. *International Journal of Production Economics, 171,* 116–133.

Katkalo, V. S., Pitelis, C. N., & Teece, D. J. (2010). Introduction: On the nature and scope of dynamic capabilities. *Industrial and Corporate Change, 19*(4), 1175–1186.

Kim, D.-Y., Kumar, V., & Kumar, U. (2012). Relationship between quality management practices and innovation. *Journal of Operations Management, 30*(4), 295–315.

Kim, Y., Choi, T. Y., & Skilton, P. F. (2015). Buyer-supplier embeddedness and patterns of innovation. *International Journal of Operations & Production Management, 35*(3), 318–345.

Knemeyer, A. M., Zinn, W., & Eroglu, C. (2009). Proactive planning for catastrophic events in supply chains. *Journal of Operations Management, 27*(2), 141–153.

Koberg, C. S., Detienne, D. R., & Heppard, K. A. (2003). An empirical test of environmental, organizational, and process factors affecting incremental and radical innovation. *The Journal of High Technology Management Research, 14*(1), 21–45.

Krolikowski, M., & Yuan, X. (2017). Friend or foe: Customer-supplier relationships and innovation. *Journal of Business Research, 78,* 53–68.

Lee, H. & Cameron, M. H. (2004). Respite care for people with dementia and their carers. *The Cochrane Library, 16*(1).

Li, C.-R., Lin, C.-J., & Chu, C.-P. (2008). The nature of market orientation and the ambidexterity of innovations. *Management Decision, 46*(7), 1002–1026.

Liu, C.-L., Shang, K.-C., Lirn, T.-C., Lai, K.-H., & Lun, Y. H. V. (2017). Supply chain resilience, firm performance, and management policies in the liner shipping industry. *Transportation Research Part A: Policy and Practice, 110,* 202–219.

Lloréns Montes, F. J., Ruiz Moreno, A. & García Morales, V. (2005). Influence of support leadership and teamwork cohesion on organizational learning, innovation and performance: an empirical examination. *Technovation, 25*(10), 1159–1172.

Mandal, S. (2012). An empirical investigation into supply chain resilience. *IUP Journal of Supply Chain Management, 9*(4), 46.

Mathisen, G. E., Einarsen, S., Jørstad, K., & Brønnick, K. S. (2004). Climate for work group creativity and innovation: Norwegian validation of the team climate inventory (TCI). *Scandinavian Journal of Psychology, 45*(5), 383–392.

Melnyk, S. A. (2014). Understanding supply chain resilience. *Supply Chain Management Review, 18*(1).

Moguilnaia, N. A., Vershinin, K. V., Sweet, M. R., Spulber, O. I., De Souza, M. M., & Narayanan, E. S. (2005). Innovation in power semiconductor industry: Past and future. *IEEE Transactions on Engineering Management, 52*(4), 429–439.

Moore, S. B., & Manring, S. L. (2009). Strategy development in small and medium sized enterprises for sustainability and increased value creation. *Journal of Cleaner Production, 17*(2), 276–282.

Nieto, M. J., & Santamaría, L. (2007). The importance of diverse collaborative networks for the novelty of product innovation. *Technovation, 27*(6), 367–377.

Nishat Faisal, M., Banwet, D. K., & Shankar, R. (2006). Supply chain risk mitigation: modeling the enablers. *Business Process Management Journal, 12*(4), 535–552.

Nishat Faisal, M., Banwet, D. K., & Shankar, R. (2007). Information risks management in supply chains: an assessment and mitigation framework. *Journal of Enterprise Information Management, 20*(6), 677–699.

Panayides, P. M., & So, M. (2005). Logistics service provider–client relationships. *Transportation Research Part E: Logistics and Transportation Review, 41*(3), 179–200.

Pettit, T. J., Fiksel, J., & Croxton, K. L. (2010). Ensuring supply chain resilience: Development of a conceptual framework. *Journal of Business Logistics, 31*(1), 1–21.

Ponis, S. T., & Koronis, E. (2012). Supply chain resilience: Definition of concept and its formative elements. *Journal of Applied Business Research, 28*(5), 921.

Ponomarov, S. Y., & Holcomb, M. C. (2009). Understanding the concept of supply chain resilience. *The International Journal of Logistics Management, 20*(1), 124–143.

Prater, E., Biehl, M., & Smith, M. A. (2001). International supply chain agility-tradeoffs between flexibility and uncertainty. *International Journal of Operations & Production Management, 21*(5/6), 823–839.

Priya Datta, P., Christopher, M., & Allen, P. (2007). Agent-based modelling of complex production/distribution systems to improve resilience. *International Journal of Logistics Research and Applications, 10*(3), 187–203.

Propris, L. D. (2002). Types of innovation and inter-firm co-operation. *Entrepreneurship & Regional Development, 14*(4), 337–353.

Raj Sinha, P., Whitman, L. E., & Malzahn, D. (2004). Methodology to mitigate supplier risk in an aerospace supply chain. *Supply Chain Management: An International Journal, 9*(2), 154–168.

Reinmoeller, P. (2005). The link between diversity and resilience. *MIT Sloan Management Review, 46*(4), 61.

Reinmoeller, P., & Van Baardwijk, N. (2005). The link between diversity and resilience. *MIT Sloan management review, 46*(4), 61.

Rice, J. B., & Caniato, F. (2003). Building a secure and resilient supply network. *Supply Chain Management Review, 7*(5), 22–30.

Ritala, P., Olander, H., Michailova, S., & Husted, K. (2015). Knowledge sharing, knowledge leaking and relative innovation performance: An empirical study. *Technovation, 35,* 22–31.

Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). New York: Free Press.

Ryan, J. C., & Tipu, S. A. A. (2013). Leadership effects on innovation propensity: A two-factor full range leadership model. *Journal of Business Research, 66*(10), 2116–2129.

Sadikoglu, E., & Zehir, C. (2010). Investigating the effects of innovation and employee performance on the relationship between total quality management practices and firm performance: An empirical study of Turkish firms. *International Journal of Production Economics, 127*(1), 13–26.

Salavou, H., & Lioukas, S. (2003). Radical product innovations in SMEs: The dominance of entrepreneurial orientation. *Creativity and Innovation Management, 12*(2), 94–108.

Santos-Vijande, M. L., & Álvarez-González, L. I. (2007). Innovativeness and organizational innovation in total quality oriented firms: The moderating role of market turbulence. *Technovation, 27*(9), 514–532.

Scholten, K., & Schilder, S. (2015). The role of collaboration in supply chain resilience. *Supply Chain Management: An International Journal, 20*(4), 471–484.

Scholten, K., Sharkey Scott, P., & Fynes, B. (2014). Mitigation processes–antecedents for building supply chain resilience. *Supply Chain Management: An International Journal, 19*(2), 211–228.
Scozzi, B., Garavelli, C., & Crowston, K. (2005). Methods for modeling and supporting innovation processes in SMEs. *European Journal of Innovation Management, 8*(1), 120–137.
Senge, P. (1990). *The fifth discipline Doubleday*. New York: Doubleday/Currency.
Sheffi, Y. (2005). Preparing for the big one [supply chain management]. *Manufacturing Engineer, 84*(5), 12–15.
Sodhi, M. S., & Lee, S. (2007). An analysis of sources of risk in the consumer electronics industry. *Journal of the Operational Research Society, 58*(11), 1430–1439.
Soni, U., Jain, V., & Kumar, S. (2014). Measuring supply chain resilience using a deterministic modeling approach. *Computers & Industrial Engineering, 74,* 11–25.
Spiegler, V. L., Naim, M. M., & Wikner, J. (2012). A control engineering approach to the assessment of supply chain resilience. *International Journal of Production Research, 50*(21), 6162–6187.
Tang, C. S. (2006). Perspectives in supply chain risk management. *International Journal of Production Economics, 103*(2), 451–488.
Tang, C., & Tomlin, B. (2008). The power of flexibility for mitigating supply chain risks. *International Journal of Production Economics, 116*(1), 12–27.
Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal, 28*(13), 1319–1350.
Tomlin, B. (2006). On the value of mitigation and contingency strategies for managing supply chain disruption risks. *Management Science, 52*(5), 639–657.
Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British Journal of Management, 14*(3), 207–222.
Un, C. A., & Asakawa, K. (2015). Types of R&D collaborations and process innovation: The benefit of collaborating upstream in the knowledge chain. *Journal of Product Innovation Management, 32*(1), 138–153.
Vaccaro, I. G., Jansen, J. J. P., Van Den Bosch, F. A. J., & Volberda, H. W. (2012). Management innovation and leadership: The moderating role of organizational size. *Journal of Management Studies, 49*(1), 28–51.
Walker, B., Gunderson, L., Kinzig, A., Folke, C., Carpenter, S., & Schultz, L. (2006). A handful of heuristics and some propositions for understanding resilience in social-ecological systems. *Ecology and society, 11*(1), 13.
Wan, D., Ong, C. H., & Lee, F. (2005). Determinants of firm innovation in Singapore. *Technovation, 25*(3), 261–268.
Wang, Z., & Wang, N. (2012). Knowledge sharing, innovation and firm performance. *Expert Systems with Applications, 39*(10), 8899–8908.
Weerawardena, J. (2003). The role of marketing capability in innovation-based competitive strategy. *Journal of strategic marketing, 11*(1), 15–35.
Wicher, P. & Lenort, R. (2012). The Ways of Creating Resilient Supply Chains [CD-ROM]. In *Proceedings of CLC* (pp. 688–694).
Wieland, A., & Marcus Wallenburg, C. (2012). Dealing with supply chain risks: Linking risk management practices and strategies to performance. *International Journal of Physical Distribution & Logistics Management, 42*(10), 887–905.
Wieland, A., & Marcus Wallenburg, C. (2013). The influence of relational competencies on supply chain resilience: a relational view. *International Journal of Physical Distribution & Logistics Management, 43*(4), 300–320.
Wilding, R. D. (2013). Supply chain temple of resilience. *Logistics & Transport Focus, 15*(11), 54–59.
Yang, B., & Yang, Y. (2010). Postponement in supply chain risk management: A complexity perspective. *International Journal of Production Research, 48*(7), 1901–1912.

Yao, Y., Kohli, R., Sherer, S. A., & Cederlund, J. (2013). Learning curves in collaborative planning, forecasting, and replenishment (CPFR) information systems: an empirical analysis from a mobile phone manufacturer. *Journal of operations management, 31*(6), 285–297.

Yilmaz Borekci, D., Rofcanin, Y., & Gürbüz, H. (2015). Organisational resilience and relational dynamics in triadic networks: A multiple case analysis. *International Journal of Production Research, 53*(22), 6839–6867.

Yoshida, D. T., Sendjaya, S., Hirst, G., & Cooper, B. (2014). Does servant leadership foster creativity and innovation? A multi-level mediation study of identification and prototypicality. *Journal of Business Research, 67*(7), 1395–1404.

Chapter 18
Supply Chain Virtualization: Facilitating Agent Trust Utilizing Blockchain Technology

Kane J. Smith and Gurpreet Dhillon

1 Introduction

With the rapid commercialization and adoption of Internet technologies by companies such as Amazon, Walmart, and Dell, a process known as *supply chain virtualization* has taken place, transforming conventional work practices across organizations. There are three key elements that represent supply chain virtualization, which include: the formation of virtual trading communities; the emergence of virtual knowledge communities; and the relocation and integration of interorganizational business processes in the cyberspace (Ho et al. 2003, 2015). The advancement of information technologies, in particular the Internet and Internet of Things (IoT), has transformed the traditional economy into a network and knowledge-based economy where electronic commerce, known as e-commerce, has assumed an increasingly important role in reshaping buyer–supplier relationships, improving core business processes, providing electronic intermediation, and reaching new segments and markets (Chandrashekar and Schary 1999; Gefen and Straub 2004; Ho et al. 2003; Verdouw et al. 2016). With the success of companies such as Amazon, significant changes are already clearly observable in retail markets in which the Web was exploited as a new channel to market, sell, and distribute consumer products (Hande and Ghosh 2015; Ho et al. 2003). However, the marketing and sales aspects of e-commerce represent only a partial understanding of the intricacies of this technological innovation, and further yet underestimate the impact it has had on management thinking and work practices (Ho et al. 2003; Verdouw et al. 2016). Hence, the impact of new technologies is not limited to a particular business process or a particular pair of trading partners as they have also created new opportunities for supply-chain reconfiguration and integration, challenging prevalent business models, processes, and relationships (Ho et al. 2003). To this end, the growing commercialization and

K. J. Smith · G. Dhillon (✉)
The University of North Carolina Greensboro, Greensboro, USA
e-mail: gpdhillon5@gmail.com

G. A. Zsidisin and M. Henke (eds.), *Revisiting Supply Chain Risk*, Springer Series in Supply Chain Management 7, https://doi.org/10.1007/978-3-030-03813-7_18

deployment of new IT-based technology across various industries, and e-commerce in particular, are driving the virtualization of supply chains and demanding new mindsets in managing these new diverse business contexts.

Supply chain virtualization can provide many distinct benefits, such as providing greater visibility within the supply chain, as the provenance of an item in a particular network can be called into question (Francisco and Swanson 2018; Korpella et al. 2017). For example, Amazon's *Fulfilled by Amazon* program offers third-party merchants an option where Amazon handles all aspects of sale, warehousing, and shipment once a seller sends their products into their warehouses (Shepard 2017). The program is designed for maximum speed as all products with the same SKUs get mixed in together, regardless of who the individual sellers who shipped them (Shepard 2017). However, this means that counterfeits can be commingled with authentic products, and even Amazon cannot easily determine where they came from. This provides an added level of protection to counterfeiters, as the smokescreen between them and the nefarious products they spike Amazon's supply chain with (Shepard 2017). This obfuscation of a product's actual origin damages the trust between Amazon, its vendors and the customers they serve. Hence, there is a need for a tool that can demonstrate the reality of a product's origin within the virtual supply chain and alleviate the issues of traceability, authenticity, transparency and ultimately trust. Therefore, the aim of such technology should be to reduce the risk of security threats to the supply chain arising from the process of virtualization.

2 Risk and Virtual Supply Chains

There are many sources of potential risk to supply chains as these sources can be any variables which cannot be predicted with certainty and from which disruptions can emerge (Juttner 2005). Per Mason-Jones and Towill (1998), five overlapping categories of supply chain risk sources exist: environmental, demand and supply, process and control risk sources. Currently, one such concern within environmental risk sources, which are comprised of any external uncertainties arising from the disruption of the supply chain such as social uncertainties via cyber-attacks like hacking (Juttner 2005). Specifically, cyber-attacks can cripple virtual supply chains as the point of entry for hackers as it is often through the weakest link in the chain (Khan and Estay 2015). The weakest link tends to be the result of the increasing complex network of the supply chain (Lu et al. 2013). For example, as global networks rely heavily on technology for supply chain efficiency and managing complexity, this in turn significantly increases their susceptibility to cyber threats (Lu et al. 2013). Hence, exacerbated by growing complexity and the need to be visible, supply chains constantly share vital streams of information and make themselves a highly lucrative target for talented hackers (Khan and Estay 2015). The implications of such cyber-attacks are financial losses, exceeding 1 trillion dollars in lost revenue annually industry-wide (Boyson 2014) and damage to brand reputation and value (Khan and Estay 2015).

To combat these threats, virtualization technologies are used to support business operations, to share information, to connect businesses, and to generate greater visibility along supply chains in order to gain knowledge and control of processes (Francisco and Swanson 2018; Khan and Estay 2015; Korpella et al. 2017). While supply chains have pursued aspects such as the standardization of business processes, increased communication, connectivity, and data exchange, the vulnerability of these systems to cyber-attacks is still rapidly increasing and responses to such threats still an emerging area of research (Boyson 2014; Khan and Estay 2015). This is due to the fact that in virtual supply chains, information is shared digitally and these supply chains are reliant on high quality information. Without it supply chain managers cannot, for example, make decisions on forecasts for production or distribution (Khan and Estay 2015). For virtual supply chains to thrive, managers must recognize that cyber-attacks are becoming common occurrences and a critical difficulty with cyber-attacks is that often a business will not know the types of cyber-risks to which it has exposure until after it has been attacked (Khan and Estay 2015).

The other categories for risk in a supply chain, per Mason-Jones and Towill (1998), are also of great interest and represent threats to an organization (Juttner 2005). For example, supply risk is the uncertainty associated with supplier activities and in general supplier relationships. As previously mentioned, Amazon's *Fulfilled by Amazon* program for third-party merchants means that counterfeits can become commingled with authentic products, and even Amazon themselves cannot easily determine where they came from (Shepard 2017); hence, counterfeiting has become a major risk in the management of virtual supply chains (Boyson 2014). This is due to the fact that there are numerous issues present in the management of virtual supply chains, which facilitate an increase in these risks (Akkermans et al. 2004; Francisco and Swanson 2018; Korpella et al. 2017). Therefore, before any potential solution to these risks can be posited; the issues related to managing such risks must be explicated and examined. Then, once this is complete, a solution can be proposed that serves to mitigate these risks by alleviating the issues related to managing them.

3 Issues in the Management of Virtual Supply Chain Risk

There are a number of difficult issues that are involved in the management of virtual supply chains. However, 3 key issues stand paramount; namely transparency, traceability, and authenticity (Akkermans et al. 2004; Francisco and Swanson 2018; Korpella et al. 2017). These are very important issues and addressing them is critical to the successful management of risk within a given virtual supply chain, such as Amazon's, which can be exploited to the chagrin of vendors, consumers and Amazon alike. Therefore, prior to exploring a potential solution to these issues, we must first understand the context of each one and how it affects supply chain virtualization within an organization. To begin, the concept of transparency in virtual supply chains will be discussed and then linked to each of the following issues before a solution is proposed that can address all of them together.

3.1 Transparency

Awaysheh and Klassen (2010) define the term transparency as the extent to which information is readily available to two or more parties in an exchange as well as to outside observers. In a supply chain context, transparency refers to information available to companies involved in a supply chain network, such as those utilized by Amazon, Walmart, or Dell. Yet, while the supply chain concept of transparency deals with the information made readily available to end users and firms in a virtual supply chain, there are varying degrees of supply chain information sharing within the supply chain (Lamming et al. 2001). Hence, transparency is important and virtual supply chains need to transparently supply all actors with knowledge, normalizing information leverage during negotiations, and providing more information about component origins and processes (Lamming et al. 2001). According to Awaysheh and Klassen (2010), transparency in the supply chain drives the adoption of socially responsible supplier practices, which serves to both influence customer purchase behavior as well as create conditions that force competitors to match their actions, especially for those with valuable, high visibility brands. For example, if a company were to source components derived from a source known to exploit its labor pool through unfair labor practices, such as Apple or perhaps Nike, consumers may choose to turn away from that brand and to their competition (Duhigg and Greenhouse 2012). Likewise, if vendors in a virtual supply chain engage in activities considered by many to be unethical, an organization can be aware of such behavior before engaging them in their network. Additionally, transparency within a virtual supply chain can help to cut down on issues of counterfeiting (Boyson 2014), a benefit to organizations whose business practices may make them more susceptible to such risks. For this reason, virtual supply chain transparency is an important issue; however, it is very difficult to ensure the transparency of a virtual supply chain network (Francisco and Swanson 2018; Korpella et al. 2017).

3.2 Traceability

Scholars have identified that optimizing transparency and traceability are correlated. Supply chain traceability leverages transparency to operationalize organizational goals related to raw material origins and provide context to a final product or service (Abeyratne and Monfared 2016; Skilton and Robinson 2009). This means that traceability is the ability to identify and verify the components, as well as the chronology of events in all steps of a process chain (Abeyratne and Monfared 2016; Skilton and Robinson 2009). The relationship between supply chain transparency and traceability is not straightforward and linear: while having more information available may lead to increased traceability, increased traceability may not lead to increased transparency if the supply chain is made of few participants with loose affiliations (Francisco and Swanson 2018). For example, traceability is hindered when material information is incomplete or missing; however, the merits of traceability are limited by the complexity within the virtual supply chain network (Abeyratne and Monfared 2016; Francisco and Swanson 2018). This means that as the complexity of a virtual supply chain network increases, it will increasingly consist of concealed elements and raise doubts around the ability of its participants to effectively and securely monitor it.

3.3 Authenticity

While transparency and traceability are correlated, authenticity is another related concept that is essential to managing virtual supply chains. Authenticity refers to the assurance that a message, transaction, or other exchange of information is from the source it claims to be from, meaning authenticity involves proof of identity. Proving authenticity occurs through the process of authentication which usually involves more than one "proof" of identity (Samonas and Coss 2014). The "proof" of identity may be something which a user knows, like a password, or a user might prove their identity with something they have, like an encrypted keycard, while modern systems can also provide proof based on something a user is (Samonas and Coss 2014). For user interaction with most systems, programs, and each other, authentication is critical, with user id and password input being the most prevalent method of authentication, but also the one to present the most problems with increased susceptibility to cyber threats such as hacking, malware, or phishing. Hence, a more complex virtual supply chain will also deal with issues surrounding its ability to deal with authentication of users to access information.

4 Reducing Risk by Building Trusting Relationships

Trust is a significant predictor of positive performance within interorganizational relationships with evidence of this extending across multiple theories of organizational research (Ireland and Webb 2007). Within transaction cost economics, for example, trust is viewed as a substitute for costly control and coordination mechanisms, while social capital theory argues that trust is a relational lubricant, allowing greater benefits of knowledge transfer, joint learning, and the sharing of risks and costs associated with exploring and exploiting opportunities (Ireland and Webb 2007). Trust is the decision to rely on a partner with the expectation that they will act according to some common agreement and at any level of trust, a certain amount of relational risk is present as that person or entity may not act according to the agreement (Ireland and Webb 2007). Firms accept elevated levels of risk to gain access to the social and economic benefits that are associated with trust-based relationships, such as trust between organizations as partners wherein an atmosphere is created in which firms willingly exceed the minimal requirements of a relationship to increase the likelihood of success for all partners (Ireland and Webb 2007).

Trust can also exist in a situation, which results in an arrangement whereby firms contribute the minimum amount of resources and time to an interorganizational relationship to achieve efficiency (Ireland and Webb 2007). With trust in a situation, a firm is willing to rely on a partner because the transaction facilitates efforts to achieve efficiency goals and the expected benefits of the transaction exceed the expected costs (Ireland and Webb 2007). This is an important concept due to the fact that virtual supply chains place trust both in situations as well as partners to maximize the efficiency of their supply chain networks and work to what is expected to be a common goal. However, when that trust is betrayed, it can be difficult to rebuild it, if it can even be earned in the first place. Hence, it is necessary for trust and trusting relationships to exist in order to achieve maximum efficiency and benefit for an organization and reduce risk within their virtual supply chain. To achieve this goal, there are 3 key drivers for building trust and trusting relationships. Therefore, by implementing a solution which utilizes and maximizes at least one of these key drivers, it can help to alleviate risk within a virtual supply chain.

4.1 Three Drivers for Trusting Relationships

When discussing trust and trusting relationships, there are 3 key mechanisms for building such relationships; formal, informal and technology. Each driver impacts trusting relationships differently and can address them in numerous different ways, yet within one of these drivers lie an opportunity for addressing all the key issues in virtual supply chain management at once. Most commonly, formal and informal mechanisms are used to build trusting relationships (Bloom and Hinrichs 2016; Bygballe et al. 2015); however, technology as a trust-building mechanism is also found in the literature and exists in technology such as online feedback systems (Ba and Pavlou 2002; Savolainen 2014). Each of these 3 drivers for building trusting relationships is unique and affects different aspects of the trusting relationship. For example, formal mechanisms are things such as contracts, whereby two (or more) parties are legally obligated to perform some set of mutually beneficial actions. In this instance, the legal contract provides a measure of trust between the two parties as they are aware that the other will perform the duties owed to the other. They can be sure of that at least so long as the penalty for not doing so does not outweigh the benefits of the required actions. This is exemplified by companies such as Dell agreeing to buy parts from multiple vendors, such as Intel, AMD, or Nvidia, to build computers to sell to consumers. It is mutually beneficial to each party to continue engaging in such a relationship, but the legal contract provides a formal mechanism to elevate levels of trust between each party that the other will keep their word. Informal mechanisms on the other hand are slightly different and often are represented in things such as individual relationships. In this instance, two organizations may enter into a formal contract, however, the individuals who interact regularly develop personal relationships. By getting to know one another, these individual relationships serve to engender greater levels of trust between the two parties, since personal relationships generate trust and discourage opportunism in economic contexts (Bloom and Hinrichs 2016). Lastly, technology can act as a trust-building mechanism for trusting relationships as it can incorporate numerous mechanisms for building trust at once (Korpela et al. 2017). For example, technology can be used to provide greater security over financial transactions, improve record keeping, and reduce process inefficiencies, which can cause issues within the supply chain and reduce vendor trust.

5 Opportunities for Creating Trusting Relationships Using Blockchain Technology

While many people may at least be tangentially familiar with Bitcoin, a decentralized digital currency, they may be much less familiar with the underlying technology that allows it to function, known as "blockchain." Bitcoin was the first real implementation of blockchain technology, invented by a mysterious developer known by the pseudonym "Satoshi Nakamoto," as the true identity or identities behind it are still unknown to this day (S. L. 2015). In the seminal work published in 2008, *Bitcoin: A Peer-to-Peer Electronic Cash System,* Satoshi Nakamoto describes the backbone of blockchain technology. It is described in the introduction as, "The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work (Nakamoto 2008)". The transactions are hashed into a single block, and all blocks make up the chain, hence, the name "blockchain." While Nakamoto was the first to successfully implement blockchain technology and make it a practical solution, they were not the first to attempt to solve what is known as the double-spending problem, which is the original purpose of blockchain in Bitcoin. The term "double-spending" dates as far back as 2007, when it was discussed by Osipkov et al. (2007) where they state, "One major attack on electronic currency is double-spending, where a user may spend an electronic coin more than once. Unless the merchant accepting the coin verifies each coin immediately, double-spending poses a significant threat." This dilemma is at the heart of the motivation for blockchain technology, and in creating a hash-based decentralized ledger system, Nakamoto solved the problem of double-spending in the Bitcoin system. Nakamoto's development of blockchain technology to solve the problem of double-spending is highly relevant in modern society and in the years since publication; others have developed non-Bitcoin uses of blockchain technology. For example, the concept of "smart contracts" as described by Bheemaiah (2015), "Smart contracts are programs that encode certain conditions and outcomes. When a transaction between 2 parties occurs, the program can verify if the product/service has been sent by the supplier. Only after verification is the sum transmitted to the suppliers account." With the advent of the post-Bitcoin blockchain landscape in 2014, referred to as "Blockchain 2.0," new technologies are being rapidly developed which take advantage of blockchain to underpin a more secure transaction ledger (Bheemaiah 2015).

5.1 What Is Blockchain?

As discussed in the previous section, blockchain was created to prevent the problem of double-spending within cryptocurrency. However, in implementation it is essentially a distributed ledger system, wherein participants work to build blocks on the chain by hashing individual transactions with the chain acting as the ledger. As a blockchain is a decentralized distributed ledger, it means that multiple participants involved in building the blocks can hold a copy of the ledger. In technical terms, every participant in the blockchain that holds a copy of the ledger is known as a "node." As all nodes hold a copy of the ledger, it means the ledger is decentralized and does not exist in a single location, which prevents a central authority from altering the ledger in any way as all nodes must "agree to" any additions to the ledger. Therefore, the most important role the nodes have is to add blocks to the chain, which is done by processing transactions (of which blocks are composed) through a one-way cryptographic hash function that cannot be altered retroactively (Iansiti and Lakhani 2017). This means that a blockchain then acts as an open and distributed ledger that records transactions between various parties in an efficient, verifiable, and permanent manner (Iansiti and Lakhani 2017). These types of secure transactions can be very appealing to any organization interested in maintaining information in a secure, yet efficient manner such as medical or banking records. A simple illustration of blockchain can be seen in Fig. 1.

Blockchain inherently provides several key technological advantages to users that are implications of its structural architecture, including; durability, transparency, immutability, and process integrity (Abeyratne and Monfared 2016; Apte and Petrovsky 2016). These key technological advantages can be exploited for the benefit of virtual supply chains. In the following Table 1, these advantages are briefly detailed.

5.2 How Can Blockchain Enable Trust in Virtual Supply Chains?

There are several benefits to virtual supply chains, which include cost-effectiveness of services and value-creating activities that are advantageous to many actors in the ecosystem, including firms and their suppliers, employees and customers (Abeyratne and Monfared 2016; Korpela et al. 2017). Hence, the effective integration between various agents within a network requires both the integration of processes and information in the supply chain (Korpela et al. 2017). Generally, coordination is achieved

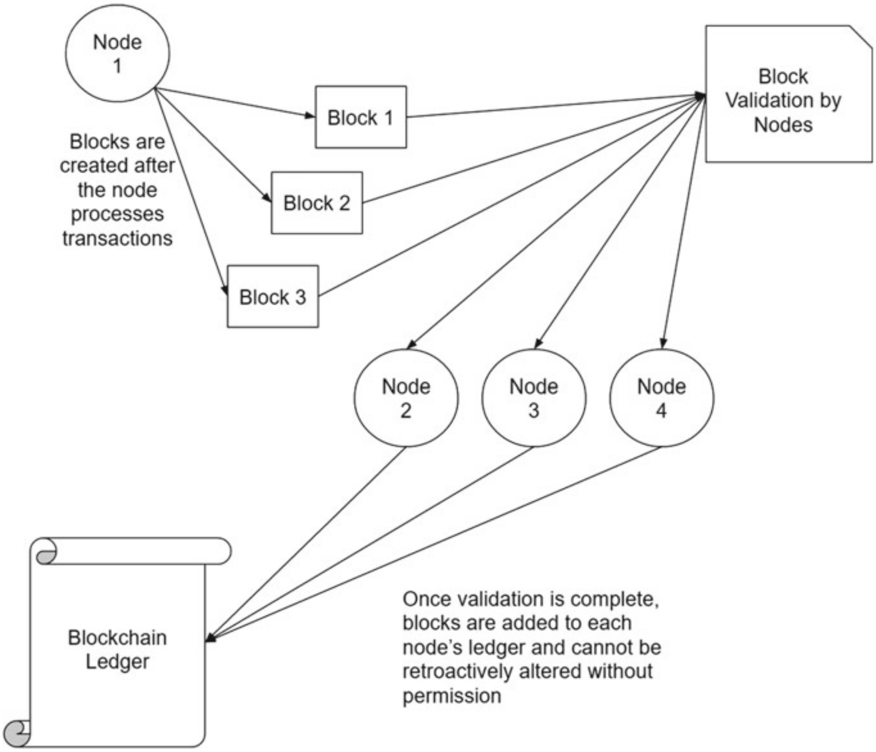


Fig. 1 Blockchain creation and validation process

by means of electronic links between information systems, enabling automated and digitalized processing of source-to-pay processes involving suppliers and customers in the supply chain (Korpela et al. 2017). However, information sharing and processing is not confined to business processes but can also include vast amounts of data from devices and sensors as well as social media. To this end, an integrated supply chain information model is essential in modern virtual supply chains, and the role of information integration is a key business driver (Abeyratne and Monfared 2016; Korpela et al. 2017). Information technology-based cost savings enable more information to be processed more accurately and more frequently, from more sources around the world, however, current technology simply focuses on where a transaction occurs and when goods, services or information are transferred across activities and systems (Korpela et al. 2017).

As global trade practices now tend to involve a range of business processes across organizational borders, new systems are required so that the information flow can be transferred electronically between agents within the virtual supply chain network in a secure and interoperable manner. Presently, two organizations may exchange supply chain documents containing important information directly via a document exchange platform; however, specialized intermediate companies are often used to

Table 1 Inherent technological advantages of blockchain technology (adapted from Abeyratne and Monfared 2016)

Advantage	Description
Durability	Decentralized networks eliminate single points of failure as opposed to centralized systems. This distribution of risk among its nodes makes blockchains much more durable than centralized systems and are better suited to deter malicious accesses
Transparency	An identical copy of a blockchain is maintained by each node on the network, allowing auditing and inspecting of the data sets in real time. This level of transparency makes network activities and operations highly visible, facilitating trust
Immutability	Data that is stored on a distributed public blockchain is practically immutable due to the need for validation by other nodes and traceability of changes. This allows users to operate with the highest degree of confidence that the chain of data is unaltered and accurate
Process integrity	Distributed open-source protocols are by nature executed exactly as written in the code. Users can be certain that actions described on the protocol are executed correctly and timely without the need for human intervention

conduct supply chain transactions (Abeyratne and Monfared 2016; Korpela et al. 2017). As well as the exchange of information, payments are typically a part of the transaction between two organizations and when financial transactions are involved, financial institutions tend to act as the intermediary or so-called trusted third parties (Abeyratne and Monfared 2016; Korpela et al. 2017). Banks typically refer to this type of work as trade finance, and it usually involves one bank for the seller and another for the buyer, which is done so that the seller's bank will provide guarantees that the seller will supply and deliver what was agreed upon by the two parties, and the buyer's bank guarantees that the buyer has received what was promised and is obligated then to pay (Korpela et al. 2017). Hence, banks are acting as a "trusted" third party, a formal mechanism, for ensuring the obligations of each party are carried through as promised. However, banks do not perform this role for free, nor are they always swift and/or efficient in carrying out this duty. To this end, blockchain technology is typically regarded as a potential means of enhancing the security and cost-effectiveness of transactions in virtual supply chains. In general, blockchain technology is used to establish integration via the Internet and conduct secure transactions quickly and at relatively low cost (Abeyratne and Monfared 2016; Korpela et al. 2017).

The characteristics of blockchains make them particularly well suited for improving supply chain transparency (Abeyratne and Monfared 2016; Apte and Petrovsky 2016; Francisco and Swanson 2018). For example, with respect to transparency, Lamming et al. (2001) describe 3 types of transparency within a supply chain network; opaque, translucent, and transparent. When information sharing between two parties in a supply chain is opaque, no information is shared between the two parties, not even day-to-day operational information. This can greatly hinder the efficiency of a supply chain in terms of cost as well as time. On the other hand, transparent supply chains share information on a selective and justified basis, which provides for maximum opportunities for collaboration and knowledge sharing to maximize efficiencies in the supply chain (Lamming et al. 2001). Hence, if the goal of a virtual supply chain is to maximize efficiencies between agents within a supply chain network, then a transparent network is ideal. Blockchain technology can help to achieve this goal as it has proven to be an effective mechanism for achieving distributed consensus in a dynamic, unreliable networked environment of untrusted participants (Francisco and Swanson 2018). This means that by turning informational assets into a digitally encoded token on a blockchain, it can be safely registered, tracked, and only traded with a private and secure key. Hence, a great deal of information can be reliably shared on a blockchain between various participants and it can be ensured that only those agents granted permission can have access, promoting greater trust of the information sharing process and increasing the likelihood of such actions.

Blockchain is also very useful for traceability applications within a virtual supply chain network, as whenever information passes from one agent to another, it is subject to counterfeiting, theft or distortion (Abeyratne and Monfared 2016; Apte and Petrovsky 2016). Again, to protect from this, blockchain technology involves the creation of a digital token, which is associated with various items within the supply chain when they are created (Abeyratne and Monfared 2016; Apte and Petrovsky 2016; Francisco and Swanson 2018). The final recipient of the information authenticates the token, which can follow the history of it to its point of origin. Hence, end users in the chain have more confidence in the information they receive since no single entity or group of entities can arbitrarily change the information contained within the blockchain. Due to most goods' linear flow from material origin to final consumer blockchain technology is, therefore, a suitable technology to facilitate supply chain traceability (Abeyratne and Monfared 2016; Francisco and Swanson 2018). Additionally, since the token enables the traceability of information within the virtual supply chain, authenticity of a sender's information can also be validated. Therefore, blockchain technology addresses all 3 of the key issues related to the management of virtual supply chains purely through its implementation, replacing the need for a formal trusted third party such as a bank. The replacement of a bank or trusted third party as an intermediary with blockchain technology then reduces costs and improves operational efficiencies within the virtual supply chain network (Abeyratne and Monfared 2016; Francisco and Swanson 2018; Korpela et al. 2017).

6 Conclusion

In this chapter, we discussed the use of blockchain technology as a mechanism for facilitating trust between various supply chain agents by addressing 3 key issues in managing virtual supply chain risk. Using blockchain technology as a distributed ledger enables various agents within the supply chain context to engage in transactions with an immutable and cryptographically secure record. This immutable and secure record serves as the foundation for a mutually beneficial relationship by engendering greater trust among supply chain agents through the reduction of varied risks within the network. The usefulness of blockchain technology is such that it enables information to be stored using a cryptographically secure hash and be distributed among multiple record-keeping nodes. Each agent within the supply chain context can act as a node and, by maintaining a copy of the record, create a distributed ledger of information. This provides two distinct benefits that facilitate trust among agents within the supply chain context; first, agents acting as nodes within the blockchain possess a copy of the information record, which cannot be altered without their consent. Second, information is stored on the blockchain using a secure method of encryption that provides protection against tampering from malicious sources and security of the information contained on the chain. Therefore, these two benefits of blockchain technology provide Supply Chain agents with powerful trust-building mechanisms, aimed at the 3 key issues related to supply chain risk. Ultimately, it is believed that this technology can extricate fear and allay concerns when dealing with risk related to virtual supply chain transparency, traceability, and authenticity issues.

References

Abeyratne, S. A., & Monfared, R. P. (2016). Blockchain ready manufacturing supply chain using distributed ledger. *International Journal of Research in Engineering and Technology, 5*(9), 1–10.

Akkermans, H., Bogerd, P., & Van Doremalen, J. (2004). Travail, transparency and trust: A case study of computer-supported collaborative supply chain planning in high-tech electronics. *European Journal of Operational Research, 153*(2), 445–456.

Apte, S., & Petrovsky, N. (2016). Will blockchain technology revolutionize excipient supply chain management? *Journal of Excipients and Food Chemicals, 7*(3), 76–78.

Awaysheh, A., & Klassen, R. D. (2010). The impact of supply chain structure on the use of supplier socially responsible practices. *International Journal of Operations & Production Management, 30*(12), 1246–1268.

Ba, S., & Pavlou, P. A. (2002). Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behavior. *MIS Quarterly, 26*(3), 243–268.

Bheemaiah, K. (2015). Blockchain 2.0: The renaissance of money. Retrieved from https://ww.ired.om/nsights/015/1/lock-hain--/.

Bloom, J. D., & Hinrichs, C. C. (2016). Informal and formal mechanisms of coordination in hybrid food value chains. *Journal of Agriculture, Food Systems, and Community Development, 1*(4), 143–156.

Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation, 34*(7), 342–353.

Bygballe, L. E., Dewulf, G., & Levitt, R. E. (2015). The interplay between formal and informal contracting in integrated project delivery. *Engineering project organization journal, 5*(1), 22–35.

Chandrashekar, A., & Schary, P. B. (1999). Toward the virtual supply chain: The convergence of IT and organization. *The International Journal of Logistics Management, 10*(2), 27–40.

Duhigg, C., & Greenhouse, S. (2012, March 29). Electronic giant vowing reforms in china plants. Retrieved from https://ww.ytimes.om/012/3/0/usiness/pple-upplier-n-hina-ledges-hanges-n-orking-onditions.tml.

Francisco, K., & Swanson, D. (2018). The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency. *Logistics, 2*(1), 2.

Gefen, D., & Straub, D. W. (2004). Consumer trust in B2C e-Commerce and the importance of social presence: Experiments in e-Products and e-Services. *Omega, 32*(6), 407–424.

Hande, P. V., & Ghosh, D. (2015). A comparative study on factors shaping buying behaviour on B2B and B2C E-commerce platforms in India. *EXCEL International Journal of Multidisciplinary Management Studies, 5*(3), 1–10.

Ho, D. C., Au, K. F., & Newton, E. (2003). The process and consequences of supply chain virtualization. *Industrial Management & Data Systems, 103*(6), 423–433.

Ho, W., Zheng, T., Yildiz, H., & Talluri, S. (2015). Supply chain risk management: A literature review. *International Journal of Production Research, 53*(16), 5031–5069.

Ireland, R. D., & Webb, J. W. (2007). A multi-theoretic perspective on trust and power in strategic supply chains. *Journal of Operations Management, 25*(2), 482–497.

Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. *Harvard Business Review, 1.*

Jüttner, U. (2005). Supply chain risk management: Understanding the business requirements from a practitioner perspective. *The International Journal of Logistics Management, 16*(1), 120–141.

Khan, O., & Estay, D. A. S. (2015). Supply chain cyber-resilience: Creating an agenda for future research. *Technology Innovation Management Review, 5*(4), 6–12.

Korpela, K., Hallikas, J., & Dahlberg, T. (2017). Digital supply chain transformation toward blockchain integration. In *Proceedings of the 50th Hawaii International Conference on System Sciences*.

Lamming, R. C., Caldwell, N. D., Harrison, D. A., & Phillips, W. (2001). Transparency in supply relationships: Concept and practice. *Journal of Supply Chain Management, 37*(3), 4–10.

Lu, T., Guo, X., Xu, B., Zhao, L., Peng, Y., & Yang, H. (2013). Next big thing in big data: The security of the ICT supply chain. In *2013 International Conference on Social Computing (SocialCom)* (pp. 1066–1073). IEEE.

Mason-Jones, R., & Towill, D. R. (1998). Shrinking the supply chain uncertainty cycle. *IOM Control,* 17–22.

Nakamoto, S. (2008, October). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://itcoin.rg/itcoin.df.

Osipkov, I., Vasserman, E., Hopper, N., & Kim, Y. (2007). Combating double-spending using cooperative P2P systems. Retrieved from http://eople.s.su.du/eyv/apers/cash-cdcs07.df.

Samonas, S., & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, *10*(3).

Savolainen, T. (2014). Trust-building in e-leadership: A case study of leaders' challenges and skills in technology-mediated interaction. *Journal of Global Business Issues, 8*(2), 45.

Shepard, W. (2017, December 21). How to avoid dangerous counterfeits on Amazon this holiday season. Retrieved from https://ww.orbes.om/ites/adeshepard/017/2/3/ow-o-rotect-our-amily-rom-angerous-akes-n-mazon-his-oliday-eason/5f5ffed7cf1.

Skilton, P. F., & Robinson, J. L. (2009). Traceability and normal accident theory: How does supply network complexity influence the traceability of adverse events? *Journal of Supply Chain Management, 45*(3), 40–53.

S. L. (2015, November 02). Who is Satoshi Nakamoto? Retrieved from http://ww.conomist.om/logs/conomist-xplains/015/1/conomist-xplains-.

Verdouw, C. N., Wolfert, J., Beulens, A. J. M., & Rialland, A. (2016). Virtualization of food supply chains with the internet of things. *Journal of Food Engineering, 176,* 128–136.

Part V
Emerging Typologies and Taxonomies

Chapter 19
Differentiating Between Supply and Supplier Risk for Better Supply Chain Risk Management

Sudipa Sarker

1 Introduction

What is the most challenging crisis in the history of Toyota? According to Liker, the installation of a wrong floor mat in a Lexus sedan by a supplier was the most challenging crisis in Toyota's history. Its consequence was that the company was vilified by the press and lost its long-held reputation for safety and quality. Clearly, such risks from suppliers can be referred to as supplier risks, and companies all over the world who are practicing either outsourcing and/or global sourcing encounter such risks time and again. However, what about the eruption of Grimsvotn—the active volcano in Iceland? This eruption led to the cancellation of over 100,000 flights, and many organizations ended up losing billions of dollars. Can this particular risk be called a supplier risk? Most probably not.

Over the years, many researchers have made significant contributions to the identification, assessment, and mitigation of supply risk. Professor Zsidisin has provided a grounded definition for this term: "Supply risk is the probability of an incident associated with inbound supply from individual supplier failures or the supply market occurring, in which its outcomes result in the inability of the purchasing firm to meet customer demand or cause threats to customer life and safety." Though much work has been carried out on supply risk, the difference between the supply and supplier risks has not been elucidated to date. In this chapter, a distinction is drawn between supply risk and supplier risk by citing examples from six cases and extant literature of supply chain risk. It is argued that drawing this distinction is necessary for the better management of the supply chain risk. The rest of the chapter is structured as follows. First, the literature on supply risk, supplier risk, supply risk management and supplier risk management are presented. Second, various supply and supplier

S. Sarker (✉)
Department of Industrial and Production Engineering, Bangladesh University of Engineering and Technology, Dhaka 1000, Bangladesh
e-mail: sudipa@ipe.buet.ac.bd

G. A. Zsidisin and M. Henke (eds.), *Revisiting Supply Chain Risk*, Springer Series in Supply Chain Management 7, https://doi.org/10.1007/978-3-030-03813-7_19

risks from six cases are presented. Third, the discussion and conclusion are drawn from the literature and cases.

2 Supply Risk

Professor Zsidisin (2003), in his definition of supply risk, has noted that managerial understanding of supply risk can be characterized by its sources and outcomes. Over the years, researchers have designated both source and its outcome as supply risk. For instance, Manuj and Mentzer (2008) refer to supply risk as a part of the supply chain risks that emerge from the network of suppliers and end at the intersection between supplier and manufacturer. In this definition, the suppliers are necessarily the source of supply risk. On the contrary, Kull and Talluri (2008) claimed that supply risks are associated with failures in delivery, cost, quality, flexibility, and general confidence. This definition of supply risk refers to the outcome aspect of risk. Again, Peck (2006) defined supply risk as "anything that disrupts or impedes the information, material or product flows from original suppliers to the delivery of the final product to the ultimate end user." This definition captures both source and outcome aspects of supply risk. The definition of supply risk adopted in this chapter is in line with Harland et al.'s (2003) definition of supply risk. They defined supply risk as the input risk that affects the inward flow of any type of resource. The rationale here is that the supply risk simply becomes the disruption in inward flow that can occur from a multitude of sources.

Table 1 lists the supply risks that pertain to the definition by Harland et al. (2003).

As evident in Table 1, a number of risks can be tagged as supply risks. For instance, the risk of unavailability of raw material can be due to the lost opportunities of production or extraction of the raw material (Liu et al. 2017), lack of availability of suppliers' raw materials (Nourbakhsh et al. 2013), and sudden price hike (Chopra and Sodhi 2014). Similarly, environment or disruption risks may also generate from a number of sources such as natural disasters (e.g., earthquake, flooding) and man-made disruptions (e.g., strikes, terrorism) (Chen et al. 2013). Again, the supply of raw materials can also be hampered during the transportation. Such risks are designated in the literature under transportation risks that may occur due to theft, delays, or re-routing during transportation. Moreover, there can be a regulatory change in the country of the buyer or supplier that may create a risk of supply of raw materials.

3 Supplier Risk

Many researchers have designated supplier risks in a multitude of ways. For instance, Aron and Clemons (2005) denoted supplier risk as the risk of opportunistic behavior from purchasing a firm's outsourcing partner. Similarly, Govindan and Jepsen (2016)

Table 1 Various supply risks extracted from the literature

Supply risks	Definitions	Reference
Unavailability of raw materials	Critical raw materials of a product are unavailable	Blengini et al. (2017)
Commodity price risk	Price volatility of commodities	Gaudenzi et al. (2018)
Acquisition risk	Risk of acquiring used products or materials	Hey (2017)
Environmental risk or disruption risk	Risk occurred in a region that may make the number of suppliers unavailable	Kamalahmadia and Paras (2017)
Supplier failures	Any type of failure of suppliers	Kull and Talluri (2008)
Competitors	Powerful competitors in the main or extended supply chain	Manuj and Mentzer (2008)
Transportation or logistics risks	Theft, pilferage, accidents, delays, damage from handling or transportation, re-routing, etc.	Radivojević and Gajović (2014); Manikandan et al. (2011)
Regulatory risk	A regulation requirement for input material	Harland et al. (2003)
Legal risk	Violation of rights, intellectual property	Finch (2004)

referred to supplier risk as the risk that the first-tier suppliers bring to the overall supply chain. They also stated that such risk is not only limited to disruptions of suppliers' operation but also includes other supply chain risks influenced by suppliers. In contrast, Jung et al. (2011) conceptualized supplier risk as a perception of the purchasing firm. They defined supplier risks as "an unexpected event that occurs from an upstream supplier and spreads to the downstream of the supply chain." This chapter adopts this definition of supplier risk. Table 2 lists the various supplier risks that pertain to this definition.

Again, it is evident from Table 2 that a number of risks are associated with upstream suppliers. For instance, suppliers could be ignorant of quality requirements of buyers. Mattel had to recall millions of toys in 2007 because of the high quantity of lead found in the paint. It should be noted that Mattel had outsourced that toy to a Chinese supplier who had a problematic subsupplier (Viswanadham and Samvedi 2013). Likewise, when a supplier is bankrupt, it may cause a significant risk to the manufacturers because many manufacturers outsource their core manufacturing to suppliers. Recently, a supplier bankruptcy shook General Motors (Walsworth 2016). Similarly, innovation incapability of the suppliers may make the buying firm suffer by imposing innovation risk (Sarker et al. 2016).

Table 2 Various supplier risks extracted from the literature

Supplier risks	Definitions	Reference
Supply quality risk	Suppliers' lack of knowledge on identifying, assessing, and managing supply risk associated with quality	Zsidisin et al. (2016)
Yield uncertainty	The yield of supplier is not reliable	Chen et al. (2015)
Unreliable supplier	Suppliers are unreliable	Tiwari et al. (2015)
High dependence on suppliers	Buyer is highly dependent on suppliers	Nguyen et al. (2017)
Innovation capability	Suppliers are not innovative enough	Sarker et al. (2016)
Technology risk	Suppliers are not technologically capable	Gualandris and Kalchschmidt (2015)
Bankruptcy risk	Suppliers' financial volatility	Valverde (2015)
Trust	Buyers do not trust suppliers	Sinha et al. (2004)
Sustainability	Suppliers have sustainability issues in their premises	Foerstl et al. (2010)
Delivery performance ability	Suppliers are not able to deliver on time and at right quantity	Hallikas et al. (2002)
Supplier capacity constraints	Suppliers do not have the capacity to meet the buyers' demand	Zsidisin et al. (2000)
Nature of source	Suppliers who are the sole source or single source for the buying firm	Christopher et al. (2011)

4 Supply Risk Management

In the literature of supply chain risk management, a multitude of methods have been proposed to manage, mitigate, or treat supply chain risks (Ho et al. 2015). Table 3 lists the various mitigation techniques for supply risks identified in Table 1.

As depicted in Table 3, there are few supply risks that can be mitigated with an intervention that involves the suppliers. For example, for supplier failures, Burke et al. (2007) advised keeping multiple sources of supply. However, there are a number of supply risks that cannot be mitigated through an intervention involving suppliers. For example, for mitigating risks of unavailability of raw materials, Blengini et al. (2017) suggested critical assessment of raw materials. Similarly, for the risk of commodity price hike, Hofmann (2011) advised centralizing commodities for leveraging on the economies of scale. Moreover, regarding the risk of material damage during transportation, Chopra and Sodhi (2004) recommended decentralization of resources in order to reduce the probability of risk occurrence as well as the sever-

Table 3 Various supplier risks extracted from the literature

Supply risks	Risk mitigation techniques	Reference
Unavailability of raw materials	Performing lifecycle assessment of critical raw materials	Blengini et al. (2017)
	Selecting a supplier that has a low risk regarding availability of raw materials	Nourbakhsh et al. (2013)
Commodity price risk	Centralizing commodity with SME suppliers	Hofmann (2011)
	Implementing various sourcing, contracting, and financing strategies	Gaudenzi et al. (2018)
Raw material acquisition risk	Design supply chain contract	Hey (2017)
Environmental risk or disruption risk	Adding redundancy by keeping multiple sources of suppliers	Kamalahmadia and Paras (2017)
Supplier failures	Practicing dual or multiple sourcing	Burke et al. (2007)
	Maintaining inventory	Mishra et al. (2016)
Competitors	Inducing flexibility	Manuj and Mentzer (2008)
Transportation or logistics risks	Decentralizing resources	Chopra and Sodhi (2004)
Regulatory risk	Change countries to source from	Viswanadham and Samvedi (2013)
Legal risk	Managing intellectual property	Finch (2004)

ity of consequences. Additionally, according to Viswanadham and Samvedi (2013), for tacking regulatory risk, it is imperative to invest in manpower who will regularly monitor countries for regulatory issues. This mitigation is especially effective when the buying firm is sourcing from developing countries such as China, India, or Bangladesh.

In summary, since many supply risks are uncontrollable and often unpredictable, the mitigation techniques for such risks are also hard to design proactively. In most cases, organizations encountering such risks need to be reactive and develop quick response systems to handle such risks.

5 Supplier Risk Management

Similar to supply risk management, a host of methods have been suggested in the literature for supplier risk management, as shown in Table 4. Unlike supply risk management, many of the techniques for supplier risk management require direct

Table 4 Various supplier risks extracted from the literature

Supplier risks	Risk mitigation techniques	Reference
Supply quality risk	Ensuring visibility in the multi-tier global supply network	Tse and Tan (2011)
Yield uncertainty	Using backup suppliers	Chen et al. (2015)
Unreliable supplier	Ordering sequentially and placing new order only when the yield from previous order is known	Tiwari et al. (2015)
High dependence on suppliers	Ensuring visibility by information technology integration between buying firms and their suppliers	Nguyen et al. (2017)
Innovation capability	Practicing single sourcing	Blome and Henke (2009)
Technology risk	Monitoring suppliers' ability to innovate	Gualandris and Kalchschmidt (2015)
Bankruptcy risk	Risk pooling through insurance	Valverde (2015)
Trust	Forming alliances	Alvarez et al. (2010)
Sustainability	Carefully selecting suppliers, phasing out suppliers that provide high non-remediable risk, and developing suppliers that provide remediable risk	Foerstl et al. (2010)
Delivery performance ability	Dual sourcing	Wang et al. (2010)
Supplier capacity constraints	Holding reserve capacity	Ellegaard (2008)
Nature of source	Re-evaluating supply base network design	Christopher et al. (2004)

interventions that involve suppliers. For instance, Tse and Tan (2011) proposed visibility in the supply network to tackle supply quality risks. They further stated that ensuring visibility requires deep integration with the suppliers. Similarly, Blome and Henke (2009) also suggested practicing single sourcing for organizations that fear innovation capability risk from suppliers. Single sourcing allows the organizations to develop a relationship with one key supplier and involve them in activities such as product development and cost minimization (Foerstl et al. 2010).

Similarly, for managing sustainability risk, the organizations carefully select suppliers who have no such issues and audit their supply base regularly for identifying a "sustainability risky" supplier. Likewise, risks such as "trust" require forming alliances with suppliers and creating win-win situations (Alvarez et al. 2010). To summarize, supplier risks can be largely handled by using interventions directed to suppliers. Since the suppliers are controllable, the risks from suppliers also become controllable to some extent.

6 Cases

Data from six different organizations from various industries are gathered, as presented in Table 5. Case I is a consumer goods giant whose data were collected from their local office in Bangladesh. For this case, five procurement professionals discussed the supply chain risks they had encountered in their work life. Case II is a leading ICT organization from Sweden. For this case, 18 procurement professionals from various levels of this organization were interviewed to understand the supply chain risks faced by these professionals. Case III is an organization that produces electromechanical locks. This organization is based in Sweden but operates globally in 70 countries. For this case, 18 procurement professionals from different locations of this organization were asked about their encounter with supply chain risk. Case IV is a leading energy industry in Sweden that is responsible for producing and distributing electricity in five different countries in Europe. For this case, four procurement professionals were interviewed to gain insights on supply chain risk relevant to this organization. Case V is the fourth leading pharmaceutical industry in Bangladesh. For this case, the head of procurement and planning was interviewed. Case VI is a small readymade garments industry in Bangladesh serving a number of customers located in Europe, USA, and Canada.

Most prevalent risks from these six cases and their mitigations techniques are noted in Table 6.

Table 6 also depicts whether the concerned risk is a supply or a supplier risk based on the understanding from the literature. Case I used to bring one key raw material from Italy that had a special type of packaging for their product. However, a vast amount of raw materials used to get wasted because of manual material handling at the port as well as at the third-party warehouses around Bangladesh. When asked to change the packaging, the supplier denied arguing that it was their standard package that was also used for countries such as Pakistan, India, and Sri Lanka. After many negotiations with the supplier, the organization could convince the supplier to change the packaging. Though the risk of wastage was mitigated with the help of the supplier, the supplier was not the source of risk in this case. Rather the supply was disrupted

Table 5 Overview of the case organizations

Cases	Nature of industries	Origin	Size (number of employees)	Operates in no. of countries
Case I	Consumer goods	UK	169,000	190
Case II	ICT	Sweden	105,852	180
Case III	Lock manufacturing industry	Sweden	45,994	70
Case IV	Energy	Sweden	20,000	5
Case V	Pharmaceutical	Bangladesh	3,485	1
Case VI	Readymade garments	Bangladesh	600	1

Table 6 Prevalent risks and their mitigation techniques

Cases	Risks	Supply	Supplier	Mitigation Techniques
Case I	Wastage due to manual material handling	√		Request the supplier to change the packaging material
	Environmental risk: Thailand flood	√		Give full order to an alternative supplier in India
	Port strike	√		Developed a local supplier
Case II	Sustainability risk		√	Performing regular sustainability audits
	Acquisition risk	√		Monitoring the market regularly
	Ash cloud in Europe	√		Incurred delay and loss even when multiple sourcing is practiced
Case III	Bankruptcy risk		√	Helping supplier to get back on feet
	Innovation risk		√	Involving suppliers for new product development
	Supplier failures		√	Switching suppliers
Case IV	Supplier Quality risk		√	Stringent quality check of requirements
	Unreliable supplier		√	Using multiple sourcing where possible
	Powerful supplier		√	Actively looking for alternative supplier
Case V	Unavailability of raw material	√		Check with other pharmaceuticals for excess quantity
	Price volatility	√		Purchase excess quantities when prices are low
	Compliance issues		√	Using suppliers approved by the end customer
Case VI	Unreliable supplier		√	Frequently switching supplier
	Suppliers' capacity constraint		√	Multiple sourcing
	Long wait of imported materials at the seaport	√		Could not be mitigated and the company had to incur loss

or lost due to the practice of manual handling of materials in Bangladesh. Thus, this risk is a supply risk and not a supplier risk. The next risk was an environmental risk that was observed during the Thailand Flood in 2011. Luckily, the organization had another supplier in India who could take on the lost ordered volume from the disrupted supplier in Thailand. The risk again is a supply risk and could be mitigated because the organization had dual sources in different countries for that particular raw material. The third prevalent risk for case I was a port strike. It is a common phenomenon to have either a strike or a long congestion at the main seaport located in Chittagong, Bangladesh. In this particular instance, the strike lasted for 40 days. Out of desperation, the company developed a local supplier for that particular raw material.

For case II, a pressing risk was sustainability risk mainly because a significant amount of sourcing was done from developing countries that had sustainability issues such as child labor and poor work environment. To tackle this risk, the case organization performed regular sustainability audits to identify and assess the extent of sustainability risk and take actions accordingly. The next prevalent risk for case II was acquisition risks. Nowadays in the ICT industry, it is a common phenomenon for small suppliers to be acquired by large suppliers in the industry. This may make the supply of raw materials uncertain because the acquirer can be a supplier with no previous relationship with the buying firm. As such risks are uncontrollable and hard to predict, companies can only mitigate risk through monitoring the market dynamics at regular intervals. This is designated as a supply risk because although the risk happens to a supplier, such risk actually hampers the supply of the raw material. The next risk for case II was due to ash clouds in Europe from the volcanic eruption in Iceland. Though the case organization was practicing multiple sourcing and had three first-tier logistics suppliers, all their logistics suppliers, unfortunately, had a common second-tier supplier. As a result, even though the supply was rerouted from air to land because of the same second-tier supplier, it was not possible to receive the supply on time. Again, this risk is a supply risk as it was not possible to predict this in advance.

All the three risks for case III were supplier risks. The first one is bankruptcy risk. The organization encountered much trouble when one of their key suppliers was bankrupted. Since the organization had much tooling investment with the supplier, the risk had to be mitigated by financially supporting the supplier. Innovation was a risk from suppliers because one of the competitive advantages of the organization was its innovation capability. The company recently made it onto the Forbes list of 100 innovative companies. So, it was elemental for the case organization to stay innovative because if the suppliers were not innovative enough, the organization was at the risk of losing its position in the list. This risk was mitigated by involving suppliers from the early stage of product development. The other risk discussed by the procurement professional was multiple supplier failures. Over the years, many suppliers had failed on cost, quality and delivery issues. Such risks were mitigated by switching from problematic suppliers to reliable suppliers.

Case IV is in a utility business that involves large power transformers. These transformers are expensive customized products built for 30–40 years. So, quality failures from suppliers were also expensive because most of these transformers were installed in remote locations; this made it both difficult and costly to replace these transformers if any issues are observed in them before their scheduled maintenance. Therefore, stringent requirements were put on the suppliers to mitigate such risk. In the technical consultant category, case IV frequently had problems with unreliable suppliers. Normally, these suppliers were "one-man" consultants who were costly but sometimes took an indefinite time to solve a problem. Case IV used multiple sourcing to tackle those unreliable technical consultants. Another difficult risk that case IV was required to manage was the risk of powerful suppliers. Due to the high technical requirements and high initial investments, most of the suppliers in the energy utility sector were large and powerful. Price negotiations with these suppliers were, therefore, extremely hard. The only way for case IV to tackle these suppliers was to look for alternative suppliers in low-cost countries.

Though case V is now a pharmaceutical organization based in Bangladesh, it once used to be owned by the global pharmaceutical giant Pfizer. Case V faced supply risks such as unavailability and price volatility of raw materials as well as compliance issues with suppliers. Unavailability of raw materials was a big concern due to the difficulty in switching raw materials in the pharmaceuticals business. This is because each raw material had to be approved in a laboratory test and sometimes with the buyer before the materials could be used for production. As a result, a sudden unavailability of raw materials directly caused production loss. Such risk was mitigated by buying from other pharmaceutical companies in the industry if they had an excess quantity. This is certainly a supply risk because raw material can be unavailable due to a number of reasons other than suppliers. Price volatility was another key risk encountered by case V because most of its raw materials were globally sourced. Depending on the availability or the unavailability of materials in the global market, the prices of certain materials varied extensively. Such risk was mitigated by purchasing quantities in excess while the prices were low. Compliance issues of suppliers were another recurrent risk for pharmaceutical industries. Even the packaging materials suppliers for the finished goods were required to meet stringent compliance requirements. Such issues were tackled by using suppliers approved by the customers.

Case VI is a small garment factory located in Bangladesh. As it was small, its suppliers were even smaller. So, the factory faced risks such as unreliable suppliers and supplier capacity constraint. Such risks were addressed by switching suppliers more frequently, especially for locally purchased materials, and using multiple sourcing for export materials. A long wait for imported materials at the port was an unavoidable and uncontrollable risk for the small garments manufacturer. Therefore, even after considering long lead times for raw materials that came from overseas, the company had no option but to pay the penalty in cases when such a risk occurred.

7 Discussion and Conclusion

This chapter sets out to create a distinction between supply and supplier risks and resonates why such distinction is needed. The findings can be subdivided into five key points.

First, supply and supplier are different units of analysis. While the supplier is an entity, supply typically refers to the raw or input materials. Many researchers have admitted that there is a confusion regarding the definition of supply risk and supplier risk (Govindan and Jepsen 2016). The authors resolved the confusion in their work by distinguishing between risk as a source or risk as a consequence. In this chapter, it is suggested that if the unit of analysis is distinguished then the risk can not only be a source or a consequence but may also have 11 other interpretations as mentioned by Aven, Renn, and Rosa. These authors claimed that risks can be defined in the following ways. Risk as "(1) expected loss; (2) expected disutility; (3) a measure of the probability and severity of adverse effects; (4) the combination of probability and extent of consequences; (5) equal to the triplet (s_i, p_i, c_i), where s_i is the *i*th scenario, p_i is the probability of that scenario, and c_i is the consequence of the *i*th scenario, $i = 1, 2, \ldots, N$; (6) uncertainty of outcome, of actions and events; (7) a situation or event where something of human value (including humans themselves) is at stake and where the outcome is uncertain; (8) an uncertain consequence of an event or an activity with respect to something that humans value; (9) the effect of uncertainty on objectives; (10) equal to the two-dimensional combination of events/consequences and associated uncertainties; and (11) uncertainty about and severity of the consequences (or outcomes) of an activity with respect to something that humans value."

Second, any source of risk such as environmental risk or transport risk that hampers the flow of raw or input materials can be designated as supply risk. In this regard, supplier failures can be a cause of supply risk because something can happen at supplier premises that might disrupt their production and/or delivery of their promised quantity to the manufacturer. In that way, the manufacturer can be short of supply because of the supplier's failure. Therefore, any risk mentioned here as supplier risks can be a source of supply risk. However, the same is not true for supplier risk. In the usual sense, the supply risk of the manufacturer will not be a supply or supplier risk for suppliers. However, it can be a demand risk for a supplier when the manufacturer decides not to order from a supplier who has failed deliveries or has some quality issues.

Third, supplier risks can emerge from any part of the supply chain because suppliers exist in all parts of the supply chain. For example, a logistics supplier as mentioned in case IV was powerful because they were a global supplier of transportation. As the supply of raw materials to the manufacturer can be brought by a logistics supplier, the manufacturer can also choose to deliver goods to the customer using the same or a different logistics supplier. In this particular case, if something bad happens to the delivery to the customer by the logistics supplier and the customer complains, the associated risk can be called a supplier risk or delivery risk but not a supply risk. Therefore, all the risks from suppliers who are downstream of the supply chain cannot be tagged as supply risks. Only the risk from upstream suppliers can be tagged as supply risk because conventionally, the supply side is known as upstream and the demand side is known as downstream.

Fourth, supplier risks are more controllable as organizations can proactively select a quality supplier, develop and grow with them, form alliances with them as well as add or remove them from the supply base when required. However, for supply risks that are not originated from suppliers, such interventions may not help to mitigate those risks.

Finally, the mitigation techniques for supply and supplier risks can vary a lot. For instance, mitigation techniques for a risk from supplier can be a change of supplier or, in extreme cases, a change of raw material that makes a supplier of a particular raw material obsolete. However, for supply risk which has not emerged from a supplier, such measures cannot be taken. For example, for causes such as delays at ports due to strikes or in case of theft or pilferage when materials are moving from one place to another, the suppliers that delivered the material or even the logistics supplier may not be the cause of those risks. Changing suppliers cannot mitigate the risk for such risks.

In conclusion, it is demonstrated in this chapter that the supply and supplier risks are treated differently in both literature and practice. It is also argued that both these risks are different on several accounts. First, the unit of analysis is different. One is raw materials; the other is suppliers. Second, a supplier can be a source of supply risk, but the opposite is not true, i.e., a supply risk to a manufacturer is typically not a source of supply risk to a supplier. Third, a supplier can exist in any part of the supply chain i.e., both upstream and downstream. On the contrary, supply risk is considered as a risk in the upstream of the supply chain. Fourth, the supplier risk is more controllable because an alternative supplier can be developed to manage the risk from a non-performing supplier. The supply risk, on the other hand, is more uncontrollable because it can happen due to a problem which is uncontrollable. For instance, it is very difficult for a manufacturer to control the unavailability of raw material due to a port strike. Finally, the mitigation techniques for both types of risks vary significantly. Future research can be directed toward performing surveys in order to generalize the differentiation between supply and supplier risks.

References

Alvarez, G., Pilbeam, C., & Wilding, R. (2010). Nestlé Nespresso AAA sustainable quality program: An investigation into the governance dynamics in a multi-stakeholder supply chain network. *Supply Chain Management: An International Journal, 15*(2), 165–182.

Blengini, G. A., et al. (2017). EU methodology for critical raw materials assessment: Policy needs and proposed solutions for incremental improvements. *Resources Policy, 53,* 12–19.

Blome, C., & Henke, M. (2009). Single versus multiple sourcing: A supply risk management perspective. In G. A. Zsidisin & B. Ritchie (Eds.), *Supply chain risk—A handbook of assessment, management, and performance 124* (pp. 125–135). New York (US): Springer.

Burke, G. J., Carrillo, J. E., & Vakharia, A. J. (2007). Single versus multiple supplier sourcing strategies. *European Journal of Operational Research, 182*(1), 95–112.

Chen, J., Sohal, A. S., & Prajogo, D. I. (2013). Supply chain operational risk mitigation: A collaborative approach. *International Journal of Production Research, 51*(7), 2186–2199.

Chen, J., Zhao, X., & Shen, Z.-J. (2015). Risk mitigation benefit from backup suppliers in the presence of the horizontal fairness concern. *Decision Sciences, 46*(4), 663–696.

Chopra, S., & Sodhi, M. S. (2004). Managing risk to avoid supply-chain breakdown. *MIT Sloan Management Review, 46*(1), 52–62.

Chopra, S., & Sodhi, M. (2014). Reducing the risk of supply chain disruptions. *MIT Sloan Management Review, 55*(3), 72–80.

Christopher, M., et al. (2011). Approaches to managing global sourcing risk. *Supply Chain Management: An International Journal, 16*(2), 67–81.

Christopher, M., Lowson, R., & Peck, H. (2004). Creating agile supply chains in the fashion industry. *International Journal of Retail & Distribution Management*, *3*(8), 367–376.

Ellegaard, C. (2008). Supply risk management in a small company perspective. *Supply Chain Management: An International Journal, 13*(6), 425–434.

Finch, P. (2004). Supply chain risk management. *Supply Chain Management: An International Journal, 9*(2), 183–196, Web. 14 Mar. 2013

Foerstl, K., et al. (2010). Managing supplier sustainability risks in a dynamically changing environment-sustainable supplier management in the chemical industry. *Journal of Purchasing and Supply Management, 16*(2), 118–130.

Gaudenzi, B., et al. (2018). An exploration of factors influencing the choice of commodity price risk mitigation strategies. *Journal of Purchasing and Supply Management January, 24*(3), 218–237.

Govindan, K., & Jepsen, M. B. (2016). Supplier risk assessment based on trapezoidal intuitionistic fuzzy numbers and ELECTRE TRI-C: A case illustration involving service suppliers. *Journal of the Operational Research Society, 67*(2), 339–376.

Gualandris, J., & Kalchschmidt, M. (2015). Supply risk management and competitive advantage: A misfit model. *The International Journal of Logistics Management, 26*(3), 459–478.

Hallikas, J., Virolainen, V.-M., & Tuominen, M. (2002). Risk analysis and assessment in network environments: A dyadic case study. *International Journal of Production Economics, 78*(1), 45–55.

Harland, C., Brenchley, R., & Walker, H. (2003). Risk in supply networks. *Journal of Purchasing and Supply Management, 9*(2), 51–62.

Hey, Y. (2017). Supply risk sharing in a closed-loop supply chain. *International Journal of Production Economics, 183*(Part A), 39–52.

Ho, W., et al. (2015). Supply chain risk management: A literature review. *International Journal of Production Research, 7543,* 1–39.

Hofmann, E. (2011). Natural hedging as a risk prophylaxis and supplier financing instrument in automotive supply chains. *Supply Chain Management: An International Journal, 16*(2), 128–141.

Jung, K., Lim, Y., & Oh, J. (2011). A model for measuring supplier risk: Do operational capability indicators enhance the prediction accuracy of supplier risk? *British Journal of Management, 22,* 609–627.

Kamalahmadia, M., & Mahour, M.-P. (2017). An assessment of supply chain disruption mitigation strategies. *International Journal of Production Economics, 184,* 210–230.

Kull, T. J., & Talluri, S. (2008). A supply risk reduction model using integrated multicriteria decision making. *IEEE Transactions on Engineering Management, 55*(3), 409–419.

Liu, J., et al. (2017). Implications from substance flow analysis, supply chain and supplier' risk evaluation in iron and steel industry in mainland China. *Resources Policy, 51,* 272–282.

Manikandan, L., Thamaraiselvan, N., & Punniyamoorthy, M. (2011). An instrument to assess supply chain risk: Establishing content validity. *International Journal of Enterprise Network Management, 4*(4), 325–343.

Manuj, I., & Mentzer, J. T. (2008). Global supply chain risk management strategies. *International Journal of Physical Distribution & Logistics Management, 38*(3), 192–223.

Mishra, D., et al. (2016). Bridging and buffering: Strategies for mitigating supply risk and improving supply chain performance. *International Journal of Production Economics, 180,* 183–197.
Nguyen, H. V., et al. (2017). Developing visibility to mitigate supplier risk: The role of power-dependence structure. *Asia-Pacific Journal of Business Administration, 9*(1), 69–82.
Nourbakhsh, V., Ahmadi, A., & Mahootchi, M. (2013). Considering supply risk for supplier selection using an integrated framework of data envelopment analysis and neural networks. *International Journal of Industrial Engineering Computations, 4*(2), 273–284.
Peck, H. (2006). Reconciling supply chain vulnerability, risk and supply chain management. *International Journal of Logistics, 9*(2), 127–142.
Radivojević, G., & Gajović, V. (2014). Supply chain risk modeling by AHP and fuzzy AHP methods. *Journal of Risk Research, 17*(3), 337–352.
Ravi, A., & Clemons, E. K. (2005). Just right outsourcing: Understanding and managing risk introduction. In *Proceedings of the 38th Hawaii International Conference on System Sciences-New York* (pp. 1–10).
Sarker, S., et al. (2016). Internal visibility of external supplier risks and the dynamics of risk management silos. *IEEE Transactions on Engineering Management, 63*(4), 451–461.
Sinha, P. R., Whitman, L. E., & Malzahn, D. (2004). Methodology to mitigate supplier risk in an aerospace supply chain. *Supply Chain Management: An International Journal, 9*(2), 154–168.
Tiwari, D., Patil, R., & Shah, J. (2015). Sequential unreliable newsboy ordering policies. *Annals of Operations Research, 233*(1), 449–463.
Tse, Y. K., & Tan, K. H. (2011). Managing product quality risk in a multi-tier global supply chain. *International Journal of Production Research, 49*(1), 139–158.
Valverde, R. (2015). An Insurance model for the protection of corporations against the bankruptcy of suppliers by using the black-scholes-merton model. *European Journal of Economics, Finance, and Administrative Sciences, 76,* 38–58.
Viswanadham, N., & Samvedi, A. (2013). Supplier selection based on supply chain ecosystem, performance and risk criteria. *International Journal of Production Research, 51*(21), 6484–6498.
Walsworth, J. (2016). GM scrambles after supplier bankruptcy. *Automotive News, 2016,* 1–10.
Wang, Y., Gilland, W., & Tomlin, B. (2010). Mitigating supply risk: Dual sourcing or process improvement? *Manufacturing & Service Operations Management, 12*(3), 489–510.
Zsidisin, G. A. (2003). A grounded definition of supply risk. *Journal of Purchasing and Supply Management, 9*(5–6), 217–224.
Zsidisin, G. A. (2016). Identifying and managing supply quality risk. *The International Journal of Logistics Management, 27*(3), 908–930.
Zsidisin, G. A., Panelli, A. & Upton, R. (2000). Purchasing organization involvement in risk assessments, contingency plans, and risk management: An exploratory study. *Supply Chain Management: An International Journal, 5*(4), 187–198.

Chapter 20
Categorizing Supply Chain Risks: Review, Integrated Typology and Future Research

Michalis Louis and Mark Pagell

1 Introduction

Supply chain risk management (SCRM) is the field that involves processes to identify, assess, treat and monitor supply chain risks so as to continuously improve the aforementioned processes to ensure constant adaptation to the changing business environment, with the ultimate objective of minimizing the probability of a supply chain risk or its corresponding losses from materializing (Sinha et al. 2004; Hallikas et al. 2004; Manuj and Mentzer 2008b; Kern et al. 2012). The topic has recently attracted the interest of many researchers (Rao and Goldsby 2009) and multiple literature reviews have been published (e.g. Colicchia and Strozzi 2012; Ho et al. 2015; Fan and Stevenson 2018a). These reviews identify the milestone studies that influenced theory development on supply chain risk management (Colicchia and Strozzi 2012), and at a more granular level, they provide a synopsis of the state-of-the-art literature in terms of risk identification, assessment, mitigation and monitoring (Ho et al. 2015).

By reviewing current SCRM research, we found a well-developed literature regarding the assessment and mitigation of supply chain risks. However, research on the identification of supply chain risks, and specifically their categorization is incomplete.

Supply chain risk identification is defined as the process of discovering, understanding, defining and categorizing supply chain risks as their early warning indicators by using appropriate methods (Hallikas et al. 2004; Sinha et al. 2004; Tummala

M. Louis (✉) · M. Pagell
Michael Smurfit Business School, University College Dublin, Dublin, Republic of Ireland
e-mail: mihalis.louis@gmail.com; michail.louis@ucdconnect.ie

M. Pagell
e-mail: mark.pagell@ucd.ie

G. A. Zsidisin and M. Henke (eds.), *Revisiting Supply Chain Risk*, Springer Series in Supply Chain Management 7, https://doi.org/10.1007/978-3-030-03813-7_20

and Schoenherr 2011; Kern et al. 2012; Kayis and Dana Karningsih 2012; Zsidisin et al. 2005; Aqlan and Lam 2015; Fan and Stevenson 2018a).

Supply chain risk identification is an important process for SCRM, because as the first step of the risk management effort (Manuj and Mentzer 2008a) it affects the quality of subsequent processes (Manuj and Mentzer 2008a). Therefore, in the case of poor supply chain risk identification the ultimate output of the supply chain risk management process will be inferior.

Current literature on supply chain risk identification offers frameworks (Trkman and McCormack 2009) and tools (Kayis and Dana Karningsih 2012) for the identification of supply chain risks. Despite the merit of these studies, more work is needed on the topic of supply chain risk categorization (a component of supply chain risk identification) for the following reasons. First, it is not clear which studies mostly impacted the development of the supply chain risk classification topic. Second, it is unknown how this development has been achieved since 2000. Third, the interactions among researchers that contributed to the topic have not yet been explicated. Last, although literature offers a plethora of overlapping supply chain risk typologies, they are incomplete and often operate at different levels of analysis.

In this chapter, we attempt to contribute to the resolution of this research gap, by focusing on the topic of supply chain risk categorization. In this manner, it will be feasible to shed light on its historical development and resolve one of the weaknesses of supply chain risk identification process in the current literature.

Hence, this chapter is divided into three sections. In the first section, we identify the most impactful studies in the supply chain risk classification topic published in peer-reviewed journals since 2000. Furthermore, we identify seminal studies that lead to the development of supply chain risk typologies as their interactions. Subsequently, we find the interactions among researchers that contributed in the supply chain risk categorization topic. In the second section, we develop a new inclusive typology of supply chain risks. Finally, the last section provides recommendations for future research.

2 Defining Risk and Supply Chain Risk

Managing risk successfully requires a well-accepted and explicit definition (Fischhoff et al. 1984). Nevertheless, there is no commonly accepted definition of risk (Rao and Goldsby 2009) which has been characterized as an elusive construct (Heckmann et al. 2015).

Two main approaches to conceptualizing risk can be noted in the literature[1] (Rao and Goldsby 2009). The first conceives of risk as a variation from expected outcomes (e.g. March and Shapira 1987). The second conceives of risk as the combination of the probability for a loss with its negative impact towards an individual or a firm (e.g. Mitchell 1995).

[1]The reader can visit the study of Rao and Goldsby (2009) for a detailed review on the risk construct.

For the purposes of this chapter, we define risk as the unwanted variation from expected outcomes that may cause losses to a firm (March and Shapira 1987; Mitchell 1995).

To define supply chain risk, we build on this definition of risk. In addition, there is ample empirical evidence to support that the materialization of supply chain risks may impose negative consequences on a focal firm. Specifically, after a set of event studies, it was found that generic disruption announcements can negatively affect shareholder value (Hendricks and Singhal 2003), stock price (Hendricks and Singhal 2005a) or operating performance (Hendricks and Singhal 2005b). Therefore, we follow Wagner and Bode (2006) and Tummala and Schoenherr (2011) to define supply chain risk[2] as the unwanted negative deviation from expected outcomes that can adversely affect supply chain operations and may result in detrimental consequences to a focal firm.

2.1 An Overview of Supply Chain Risk Management (SCRM) Literature

The field of supply chain risk management (SCRM) involves processes for the identification, assessment, treatment and monitoring of supply chain risks so as to continuously improve the aforementioned processes to ensure constant adaptation with the changing business environment, with the ultimate objective of minimizing the probability of a supply chain risk or its corresponding losses from materializing (Sinha et al. 2004; Hallikas et al. 2004; Manuj and Mentzer 2008b; Kern et al. 2012). In this manner, supply chain risks are identified and assessed under a structured approach by using specific tools or methods. This should then allow managers to address supply chain risks by implementing appropriate strategies to minimize the probability of a supply chain risk or its corresponding losses materializing (Norrman and Jansson 2004; Manuj and Mentzer 2008a). Authors contributing to the discourse of supply chain risk management focus on identification, assessment and mitigation. Assessment and mitigation are well studied. For instance, several studies offered insights on the assessment of risks in the upstream supply chain (e.g. Zsidisin et al. 2004) and identified contextual factors that affect visibility in the downstream supply chain (e.g. Smaros et al. 2003). Additionally, the literature offers a plethora of valuable qualitative and quantitative approaches to understand and mitigate risk in volatile environments in the upstream (e.g. Constantino and Pellegrino 2010) and downstream supply chain (Xiao and Yang 2008). Finally, a few studies offer valuable insights regarding the negative impact of supply chain risks on supply chain performance (Wagner and Bode 2008; Chen and Wu 2013).

However, only a few studies have contributed to the identification of supply chain risks (e.g. Neiger et al. 2009; Zsidisin et al. 2016). Thus, current literature is incomplete regarding supply chain risk identification and specifically the categorization of

[2]The reader can visit the study of Ho et al. (2015) for a detailed review on the supply chain risk construct.

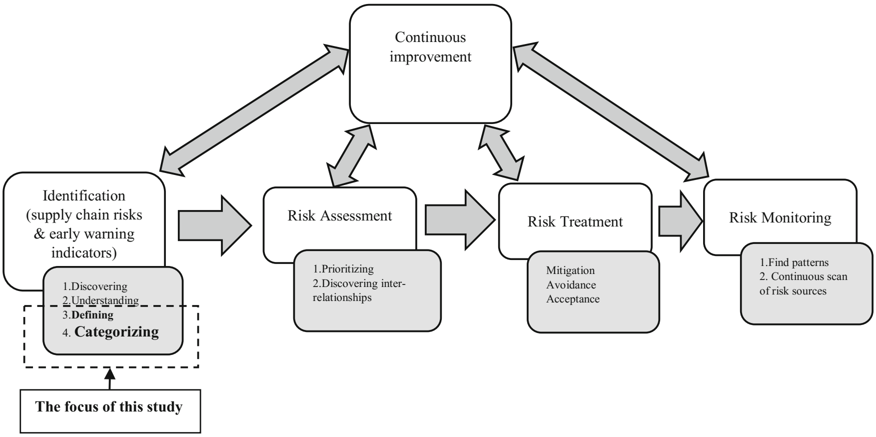


Fig. 1 Focus of this study (based on Table 1)

supply chain risks (Rangel et al. 2015). Risks come in many forms, and thus, different approaches (Zsidisin and Wagner 2010) are required for their identification. Firms that are aware of the types of risks they confront in the supply chain can improve the management of these risks (Chopra and Sodhi 2004). However, the field of supply chain risk management has been characterized as unclear and disorganized (Lavastre et al. 2014) making it difficult for firms to develop meaningful risk categorizations that are specific to their environment.

Therefore, the focus of our study is indicated by Fig. 1. The figure depicts the importance of risk identification which has been well documented in the literature (e.g. Hallikas et al. 2004; Kern et al. 2012). Risk identification determines the quality of the overall risk management effort (Hallikas et al. 2004; Neiger et al. 2009; Kayis and Dana Karningsih 2012; Kern et al. 2012) by informing subsequent processes (Kern et al. 2012). Below, we review the literature on supply chain risk identification.

2.2 Supply Chain Risk Identification

For the purposes of this chapter, we define supply chain risk identification by synthesizing current definitions (Hallikas et al. 2004; Sinha et al. 2004; Tummala and Schoenherr 2011; Kern et al. 2012; Kayis and Dana Karningsih 2012; Zsidisin et al. 2005; Aqlan and Lam 2015; Fan and Stevenson 2018a) as: the process of discovering, understanding, defining and categorizing supply chain risks as their early warning indicators by using appropriate methods (Fig. 1).

Current literature on supply chain risk identification offers a wide array of approaches to identify risks such as structured methods (van der Vorst and Beulens 2002; Gaudenzi and Borghesi 2006), methodologies (Adhitya et al. 2009; Neiger

Table 1 Processes of supply chain risk management

SCRM process	Definition	References
Risk identification	The process of discovering, understanding, defining and classifying supply chain risks according to specific criteria (e.g. sources) as their early warning indicators by using appropriate methods	Hallikas et al. (2004), Sinha et al. (2004), Tummala and Schoenherr (2011), Kern et al. (2012), Kayis and Dana Karningsih (2012), Zsidisin et al. (2005), Aqlan and Lam (2015), Fan and Stevenson (2018a)
Risk assessment	The process of prioritizing and discovering potential interrelationships of identified supply chain risks according to the probability and impact using qualitative or quantitative methods	Zsidisin et al. (2000), Hallikas et al. (2004), Gaudenzi and Borghesi (2006), Tummala and Schoenherr (2011)
Risk treatment	The process of selecting and implementing appropriate strategies (e.g. mitigation, avoidance, transfer) with the objective to reduce either the probability or impact of a supply chain risk	Zsidisin et al. (2005), Manuj and Mentzer (2008a, b), Kern et al. (2012), Giannakis and Papadopoulos (2016), Fan and Stevenson (2018a)
Risk monitoring	The process that aims to find potential patterns in the supply chain risk dimensions (e.g. probability) by continuously scanning sources of supply chain risk	Hallikas et al. (2004), Zsidisin et al. (2005)
Continuous improvement	The process that entails the effectiveness and the control of all the measures associated with supply chain risk management to ensure constant adaptation to the changing business environment	Sinha et al. (2004), Manuj and Mentzer (2008a), Kern et al. (2012)

et al. 2009), approaches (Christopher and Peck 2004; Trkman and McCormack 2009) and tools (Kayis and Dana Karningsih 2012). It should also be noted that in recent years research has begun to focus on supply chain risks associated with sustainability (Busse et al. 2017) and quality (Zsidisin et al. 2016). The identification of supply chain risks has been explored in multiple industries such as food (Busse et al. 2017), medical (Gaudenzi and Borghesi 2006) and automotive (Trkman and McCormack 2009). Despite the merit of these studies, the literature is immature (Rao and Goldsby 2009; Fan and Stevenson 2018b) and there is a need for a better understanding of supply chain risk categorization for two reasons. First, its historical development has never been explained, creating a "black box" for both researchers and practitioners. Second, and more important, the literature offers a plethora of overlapping supply chain risk typologies, which are incomplete. As Fig. 1 suggests, this weakness is important because if the development of categories is not inclusive, it may hinder risk identification and negatively affect the quality of the output of subsequent processes. In essence, the quality of supply chain risk categorization may affect the overall quality of risk management effort.

Therefore, this chapter focuses on the process of supply chain risk identification; specifically, its sub-domain supply chain risk classification.

This study answers the following questions on supply chain risk classification:

1. What are the most influential studies on the topic of supply chain risk classification?
2. How has the supply chain risk classification topic developed over time?
3. What are the interactions among researchers that contributed to the topic of supply chain risk classification?
4. How can consensus be achieved across the supply chain risk classification studies published since 2000?

3 Research Methodology

Figure 2 depicts the research methodology of this study which is based on the following structured literature review approaches (Denyer and Tranfield 2009; Colicchia and Strozzi 2012; Rangel et al. 2015; Fan and Stevenson 2018a) and involves seven steps.

4 Results

4.1 What Are the Most Influential Studies on the Topic of Supply Chain Risk Classification (RQ1)

Despite the merit of previous studies that offer classifications of supply chain risk (e.g. Harland et al. 2003; Chopra and Sodhi 2004) their impact to SCRM field has not yet been evaluated by using bibliometric measures. This suggests a potential limiting factor at the efforts of early stage researchers to find seminal studies on the topic which may hinder their research outcomes, and ultimately the development of supply chain risk classifications. To the best of our knowledge, only the study conducted by Colicchia and Strozzi (2012) applied a structured methodology to measure the impact of SCRM studies. However, there was no specificity towards the supply chain risk classification topic.

Hence, answering RQ1 will benefit the efforts of both early stage and experienced researchers looking to further develop the topic. Thus, this study uses two bibliometric measures to capture the level of impact both from a general audience point of view (global citation score) and closeness centrality.

Step 1: Formulation of research questions	
Research Questions	Research gap
Systematic Literature Network Analysis Research Questions (SLNA) *RQ1*. What are the most influential studies on the topic of supply chain risk classification?	The impact of supply chain risk classifications studies is not clear making it difficult for early stage researchers to evaluate the importance of these studies.
RQ2. How has the supply chain risk classification topic developed over time?	The literature is lacking a dynamic perspective on the development of the supply chain risk classification topic.
RQ3. What are the interactions among researchers that contributed in the topic of supply chain risk classification?	Interactions among researchers that contributed to the topic have not yet been explicated.
RQ4. How can consensus be achieved across the supply chain risk classification studies published since 2000?	Existing classifications overlap and yet are incomplete.

Step 2: Keyword search	
The keywords used to search the abstract, main body, and the keywords set by the artilces's authors.	
Criteria	Explanation
1. Keywords: a) "supply chain" or "supply" and "risk sources" b) "supply chain" or "supply" and "risk" and "taxonomy" or "typology", c) "supply chain" or "supply" and "risk domain", d) "supply chain" or "supply" and "risk" and "classification" or "categorization", e) "Supply" or "Supply chain" and "risk scopes", f) "supply" or "supply chain and "disruptions" and "sources" g) "supply chain risk", and "Vulnerability" and "sources" or "classification" or "typology" or "taxonomy" h) "supply" or "supply chain" and "risk factors" or "risk drivers" i) "Supply" or "supply chain" and identification	a) Used as a construct to classify supply chain risks (Jüttner et al. 2003), b) Differences explained by Wagner and Bode (2006), c) Used to refer to supply chain risk classifications (Bandaly et al. 2012), d) Used to refer to the topic of supply chain risk categorizations (e.g. Colicchia and Strozzi 2012, Guertler and Spinler 2015, Rangel et al. 2015), e) Used to refer to the topic of supply chain risk categorizations (Sodhi et al. 2012), f) To discover additional sources of supply chain risk. g) Used to refer to supply chain risk classifications by Wanger and Bode (2006). h) Used by some authors as associative to the topic of supply chain risk classifications (e.g. Chopra and Sodhi, 2004; Canbolat et al. 2007).

Fig. 2 Research methodology (adapted from Denyer and Tranfield 2009; Colicchia and Strozzi 2012; Rangel et al. 2015; Fan and Stevenson 2018a)

j) "supply" or "supply chain" and "risk types"	i) As Figure 20.1 suggests supply chain risk classification is a sub-part of supply chain risk identification. j) Used by some authors to refer to the topic of supply chain risk categorization (e.g. Tang and Tomlin 2008).
2. Web of Science database & Business source complete database (EBSCO)	Offers the best coverage of operations and supply chain management literature (Fan and Stevenson 2018a).
3. Selection period: 2000 – 2017	Supply chain risk management has mainly attracted the interest of researchers since 2000 (Colicchia and Strozzi, 2012, Ho et al. 2015).

Step 3: Assessment of quality and relevance	
Criteria	Explanation
1. Articles that are not published in peer – reviewed journals and not written in English were excluded.	Peer review process associates to high quality standards (Light and Pillemer 1984).
2. After reviewing the title and abstract of each article, articles with no relevancy were removed.	As applied by Fan and Stevenson (2018a) to ensure relevancy.
3. After full text scanning articles marginally relevant were removed.	As applied by Fan and Stevenson (2018a) to ensure adequacy conducting a literature review about supply chain risk management.
4. During full text scanning, relevant articles were added using a snowball approach.	To ensure that relevant articles will be included in this literature review, even if they do not meet selected keywords.

Step 4: Conducting Citation network analysis
1. Citation & popularity (GCS) data were downloaded from Web of Science for each article. This captures the impact of each article for a general audience and specifically to the topic of supply chain risk categorization by using the measure of input closeness centrality (RQ1) (Colicchia and Strozzi 2012). 2. Available data were imported to Histcite. These data were converted to network level data (Colicchia and Strozzi 2012). At this stage, GCS measure was visible for most of the studies. 3. Network level data were imported to Gephi. This allowed for the manual insertion of

Fig. 2 (continued)

citation data for studies that were not available from Web of Science. Furthermore, it allowed the manipulation of data at a node level.

4. The citation network was imported to Pajek to calculate the input closeness centrality measure (RQ1), that captures the importance of a node within a network (Colicchia and Strozzi, 2012).

⇩

Step 5: Identification of the development of the topic over time.

1. To identify how supply chain risk categorization developed over time (RQ2) we performed a main path analysis.
2. Traversal weights of studies and citations were quantified by using the three methods included in Pajek (search path count, search path link count, search path node pair)[3] (Colicchia and Strozzi, 2012).
3. A local for main path analysis was used instead of a global one, because RQ2 implies the examination of progressing significance, which can only be achieved by using a local approach (Liu and Lu, 2012).
4. We denoted a forward orientation to the analysis, to capture unique contributions in the topic of supply chain risk categorization. According to Liu and Lu (2012) this can be achieved by denoting a forward orientation to the main path analysis.
5. We set the degree of tolerance to (0.44) that closely approximates to the default tolerance.

⇩

Step 6: Identification of researcher communities in the supply chain risk categorization topic

1. To identify interactions among researchers (RQ3) we used a clustering algorithm (Louvain simple method) in pajek.
2. We select this method because it is the simplest to identify communities (Aynaud and Guillaume, 2010) thus it is exempted from biases.

⇩

Step 7: Analysis, coding & clustering risks

1. To answer RQ4 the following steps were implemented.
2. Using a Microsoft excel spreadsheet each risk type terminology and definition were captured by two columns.
3. The risk clusters used used by Rangel et al. (2015), was used as a starting point to allocate risk types to appropriate risk clusters based on definitions similarity. From this, new definitions and risk clusters appeared relative to Rangel et al. (2015).
4. New risk clusters were formed when there was no fit with Rangel et al. (2015) classification.
5. For each risk cluster articulated it was tried to achieve consensus for the risk type demonstrating the highest frequency of appearance.
6. In the case, it was not possible to articulate a risk cluser relative risk types were moved to the risk cluster entitled as "other".

[3]The reader may visit Colicchia and Strozzi (2012) for a details regarding the systematic literature network analysis method.

Fig. 2 (continued)

Table 2 lists the fifteen most impactful studies that categorize supply chain risks based on their global citation score (GCS), which quantifies the total number of citations a study received from studies that are not contained in the network (Colicchia and Strozzi 2012). From the left side to the right, Table 2 indicates the ranking of a study in terms of GCS, the title of the study, the authors, the journal the study was published in, the relevant GCS measure, and the cluster of researchers the study was allocated to, using the Louvain algorithm. For instance, the study “Perspectives in supply chain risk management” was authored by C. S. Tang published in the “International Journal of Production Economics” in 2006 and it has been allocated by the algorithm to the community cluster one. This article is ranked first because it enjoys the highest GCS score.

Table 2 Ranking of the top fifteen articles according to global citation score (GCS) measure (Created using HistCite from Clarivate Analytics)

Rank	Title	Author	Journal/Year	GCS	Cluster
1	Perspectives in supply chain risk management	Tang CS	*International Journal of Production Economics (2006)*	662	1
2	Managing disruption risks in supply chains	Kleindorfer PR, Saad GH	*Production and Operations Management (2005)*	569	3
3	Managing risk to avoid supply chain breakdown	Chopra S, Sodhi MS	*MIT Sloan Management Review (2004)*	505	3
4	A supply chain view of the resilient enterprise	Sheffi Y, Rice JB	*MIT Sloan Management Review (2005)*	302	4
5	Global supply chain risk management strategies	Manuj I, Mentzer JT	*International Journal of Physical Distribution & Logistics Management (2008)*	223	6
6	Risk management processes in supplier networks	Hallikas J, Karvonen I, Pulkkinen U, Virolainen VM, Tuominen M	*International Journal of Production Economics (2004)*	222	1
7	The design of robust value-creating supply chain networks: a critical review	Klibi W, Martel A, Guitouni A	*European Journal of Operational Research (2010)*	221	3

(continued)

Table 2 (continued)

Rank	Title	Author	Journal/Year	GCS	Cluster
8	The power of flexibility for mitigating supply chain risks	Tang C, Tomlin B	*International Journal of Production Economics (2008)*	212	3
9	Global supply chain risk management	Manuj I, Mentzer JT	*Journal of Business Logistics (2008)*	191	3
10	An empirical examination of supply chain performance along several dimension of risk	Wagner SM, Bode C	*Journal of Business Logistics (2008)*	187	4
11	Identifying risk issues and research advancements in supply chain risk management	Tang O, Musa SN	*International Journal of Production Economics (2011)*	173	3
12	Supply chain risks: a review and typology	Rao S, Goldsby TJ	*The International Journal of Logistics Management (2009)*	156	4
13	Ensuring supply chain resilience: development of a conceptual framework	Pettit TJ, Fiksel J, Croxton KL	*Journal of Business Logistics (2010)*	144	6
14	The importance of decoupling recurrent and disruption risks in a supply chain	Chopra S, Reinhardt G, Mohan U	*Naval Research Logistics (2007)*	135	3
15	Supply chain risk in turbulent environments—a conceptual model for managing supply chain network risk	Trkman P, McCormack K	*International Journal of Production Economics (2009)*	132	1

Table 3 depicts the top fifteen studies in terms of closeness centrality. Closeness centrality captures the influence of a specific node/study in terms of knowledge development; by considering the total times, it is cited by other nodes/studies in the network (Colicchia and Strozzi 2012). For instance, the conceptual study conducted by Chopra and Sodhi (2004) is the most influential in the network because it has the highest closeness centrality score.

From Tables 2 and 3, it can be noted that a small number of authors (Chopra and Sodhi 2004; Kleindorfer and Saad 2005; Christopher S. Tang 2006; Hallikas et al. 2004) contributed multiple impactful studies. These four studies contributed to both

Table 3 Ranking of the top fifteen articles according to closeness centrality (Created using HistCite from Clarivate Analytics and Pajek)

Rank	Title	Author	Journal/year	Closeness centrality	Cluster
1	Managing risk to avoid supply chain breakdown	Chopra S, Sodhi MS	*MIT Sloan Management Review (2004)*	0.536667	3
2	Risk in supply networks	Harland C, Brenchley R, Walker H	*Journal of Purchasing & Supply Management (2003)*	0.487179	2
3	Managing disruption risks in supply chains	Kleindorfer PR, Saad GH	*Production and Operations Management (2005)*	0.467416	3
4	Ericsson's proactive supply chain risk management approach after a serious sub-supplier accident	Norrman A, Jansson U	*International Journal of Physical Distribution & Logistics Management (2004)*	0.461709	4
5	A conceptual framework for the analysis of vulnerability in supply chains	Svensson G	*International Journal of Physical Distribution & Logistics Management (2000)*	0.450728	4
6	Supply chain risk management: understanding the business requirements from a practitioner perspective	Jüttner U, Peck H, Christopher M	*The International Journal of Logistics Management (2003)*	0.42932	4
7	Mitigating supply chain risk through improved confidence	Christopher M, Lee H	*International Journal of Physical Distribution & Logistics Management (2004)*	0.427317	2

(continued)

Table 3 (continued)

Rank	Title	Author	Journal/year	Closeness centrality	Cluster
8	Perspectives in supply chain risk management	Tang CS	*International Journal of Production Economics (2006)*	0.4256	1
9	Managerial perceptions of supply risk	Zsidisin GA	*Journal of Supply Chain Management (2003)*	0.404308	2
10	Risky business: expanding the discussion on risk and the extended enterprise	Spekman RE, Davis EW	*International Journal of Physical Distribution & Logistics Management (2004)*	0.360211	2
11	Risk management processes in supplier networks	Hallikas J, Karvonen I, Pulkkinen U, Virolainen VM, Tuominen M	*International Journal of Production Economics (2004)*	0.346067	1
12	Supply chain risk management understanding the business requirements from a practitioner perspective	Jüttner U	*The International Journal of Logistics Management (2005)*	0.332791	4
13	An agency theory investigation of supply risk management	Zsidisin GA, Ellram LM	*Journal of Supply Chain Management (2003)*	0.331754	2
14	Building the resilient supply chain	Christopher M, Peck H	*The International Journal of Logistics Management (2004)*	0.328966	6
15	Securing the upstream supply chain: a risk management approach	Giunipero LC, Eltantawy RA	*International Journal of Physical Distribution & Logistics Management (2004)*	0.311087	4

the supply chain risk classification topic and they demonstrate a significant impact towards a general audience.

The point here is that from an author's point of view about 26 studies (excluding duplicates in Tables 2 and 3) were the most impactful to the supply chain risk classification topic demonstrating the highest bibliometric measures (GCS, closeness centrality). Despite the fact that these results capture the level of contribution from an author's point of view, they do not capture potential interactions among researchers, which may also benefit researchers. This constitutes a motivation of RQ3 that will attempt to identify potential interactions among researchers.

4.2 *How Has the Supply Chain Risk Classification Topic Developed Over Time? (RQ2)*

The literature lacks a dynamic perspective that captures the development of the supply chain risk classification topic. By addressing this research gap in the literature, we hope to identify milestone studies that contributed to the development of the topic at different points in time. Thus, by answering RQ2 we aim to offer a dynamic perspective on the development of this field.

In this section, the development of the supply chain risk classification topic will be reviewed in terms of (a) the use of risk factors in the classification scheme, (b) the application of classification criteria, (c) the identification of milestone studies in the development of supply chain risk classification topic.

Figure 3 depicts the distribution of scientific articles within the supply chain risk classification topic published in peer-reviewed journals since 2000, using Fan and Stevenson's (2018a) coding scheme. The number of studies that encompass

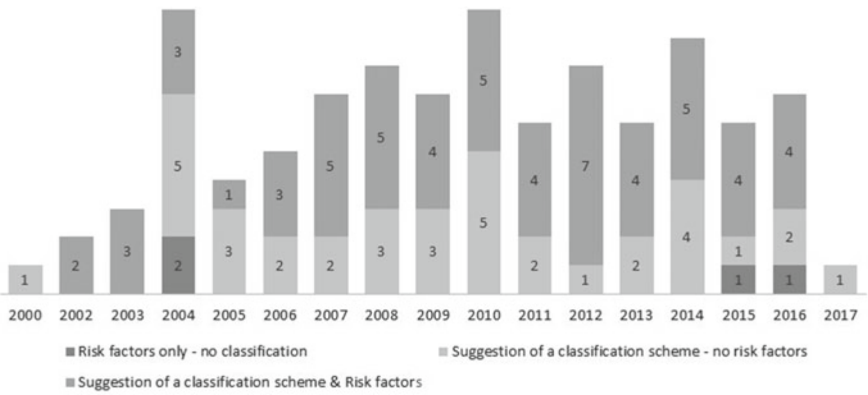


Fig. 3 Distribution of scientific articles within the topic of supply chain risk classifications published during the period 2000–2017

supply chain risk classifications has grown; however, a key conclusion from this development is that none of the existing typologies is complete, though most overlap. The formation of consensus among researchers on supply chain risk classifications has been fragmented both from the suggestion of classification schemes without risk factors and the use of different criteria to classify supply chain risks over time. Specifically, 37% of the studies reviewed for the purposes of this chapter suggested classification schemes without risk factors (Fig. 3).

Furthermore, a plethora of criteria have been used by researchers since 2000 to classify supply chain risks. Table 4 indicates the criteria used by researchers since 2000 as higher order constructs for a first time, to classify supply chain risks such as locality (e.g. Christopher and Peck 2004). Despite the fact, a plethora of different criteria has been used since 2000, certain criteria have been used inconsistently or sparsely. This may hinder managerial decision risk making because managers tend to be idiosyncratic in understanding risk (March and Shapira 1987). For instance, intentionality is used by only one study as a higher order construct (Stecke and Kumar 2009).

We conducted a main path analysis to identify milestone studies in the development of supply chain risk classification topic and offer a dynamic perspective on how the literature developed (e.g. Colicchia and Strozzi 2012; De Nooy et al. 2011). Figure 4 depicts the results of this analysis, while the size of the arrows indicates the level of the impact of each study.

The main path analysis results suggest three stages of development in the supply chain risk classification scheme literature.

First stage (2000–2004). The major characteristic of this stage is the development of the first classification schemes that delineate between sources that are internal to the firm, internal to the supply chain and external to the supply chain. A first categorization of supply chain risks according to the ability to be quantified is established (Svensson 2000). Researchers also start to address problems associated with relational and competitiveness issues. For instance, Harland et al. (2003) include supply and consumer-related risk sources in addition to issues arising internally to the firm or externally to the supply chain, while Jüttner et al. (2003) include relational (chaos, lack of ownership) and competitiveness issues (inertia).

Second stage (2005–2012). The major characteristics of this stage are the further understanding of network risk sources (e.g. Peck 2005; Lockamy and McCormack 2010), the incorporation of theories to inform supply chain risk categorizations, and the clear delineation of supply chain risks. For instance, Peck (2005) uses a theory for a first time (network theory) that considers interdependencies among supply chain risks. The studies of Wagner and Bode (2006, 2008) offer clearly delineated definitions and capture rare but severe risks emanating externally to the supply chain, which are labelled as catastrophic. At this stage, it was noted that literature had developed as separated silos, and thus a synthesis of the literature was in high demand. This demand was met by Rao and Goldsby (2009) who were the first to synthesize the generic risk literature in the context of supply chains. These authors build on the work of Ritchie and Marshall (1993) to develop a generic typology of supply chain

Table 4 Development of the supply chain risk classifications in terms of criteria used

Year	Criterion	Risk categorization	Reference
2004	Locality	• Internal to the firm • Internal to the supply chain • External to the network	Christopher and Peck
2004	Quantification ability	• Foreseen (e.g. measurable by statistical data) • Perceived (e.g. sensed by intuition)	Sinha et al.
2005	Consequence severity	• Operational (e.g. coordination of supply and demand) • Disruptive (e.g. natural disasters)	Kleindorder and Saad
2006	Controllability	• Controllable • Partially controllable • Uncontrollable	Wu et al.
2007	Extent of global operations	• Primary global • Not specifically global • Exacerbated by global supply chain	Canbolat et al.
2007	Level of decision-making	• Strategic (e.g. reputation, capacity) • Operational (e.g. supplier delays, inventory)	Sodhi and Lee
2007	Frequency	• Disruption • Recurrent	Chopra et al.
2009	Probability and impact	• High likelihood, low impact risks • Low likelihood, high impact risks	Oke and Gopalakrishnan
2009	Intentionality	• Intentional (e.g. terrorism) • Unintentional	Stecke and Kumar
2011	Flows	• Material • Financial • Information	Tang and Musa
2014	Newness	• Ordinary • Sustainability	Hofmann et al.
2015	SCOR model	• Plan • Source • Make • Deliver • Return	Rangel et al.

Fig. 4 Main path analysis

risks dividing them into environmental, industry, organizational, problem-specific and decision-maker.

Third stage (2013–2016). This period is characterized by more systematic efforts to categorize supply chain risks. On the one side, Ho et al. (2015) offer a categorization of supply chain risks by using systematic literature review method. On the other side, the study of Dong and Cooper (2016) represents a stream of literature that uses quantitative methods to categorize supply chain risks according to probability and impact. They categorize supply chain risks into critical, high, intermediate and low risks, adding nuance to the propositions offered by Oke and Gopalakrishnan (2009) that divided supply chain risks into two broad categories: high likelihood, low impact and low likelihood, high impact events.

By applying a local forward approach, we identified the antecedents of important contributions in the supply chain risk classification topic by relying on uniqueness instead of focusing on studies that adopted ideas from a wide range of sources (Liu and Lu 2012). We distinguished this development into three historical stages and found that uniqueness of these studies relies on empirical driven results by focusing on multiple levels and use of theories to inform their results. Furthermore, these studies provide clear-cut definitions and include adequate risk factors to develop classification schemes. Last, they use quantitative approaches to categorize supply chain risk according to probability and impact.

4.3 What Are the Interactions Among Researchers that Contributed to the Topic of Supply Chain Risk Classification? (RQ3)

Numerous studies published since 2000 have offered supply chain risk classifications (e.g. Zsidisin 2003a; Zsidisin and Ellram 2003; Wagner and Bode 2008). However, it is unknown how the authors who contributed to these studies interact to form communities. By answering RQ3, we identify different communities of researchers that formed over years, providing valuable insight into the topic's status quo.

Figure 5 depicts the different communities of researchers that contributed in the supply chain risk classification topic. To identify the different communities of researchers, all the selected studies for the purposes of this review were clustered using a Pajek's clustering algorithm. These clusters indicate different communities among researchers because they are internally constituted from more relationships than externally (Mrvar and Batagelj 2018).

Table 5 depicts the contributions of each researcher community cluster according to the following criteria:

- The frequency of studies contributed by a researcher community cluster at the top 15 in the GCS ranking (Table 2).
- The frequency of studies contributed by a researcher community cluster at the top 15 in the closeness centrality ranking (Table 3).

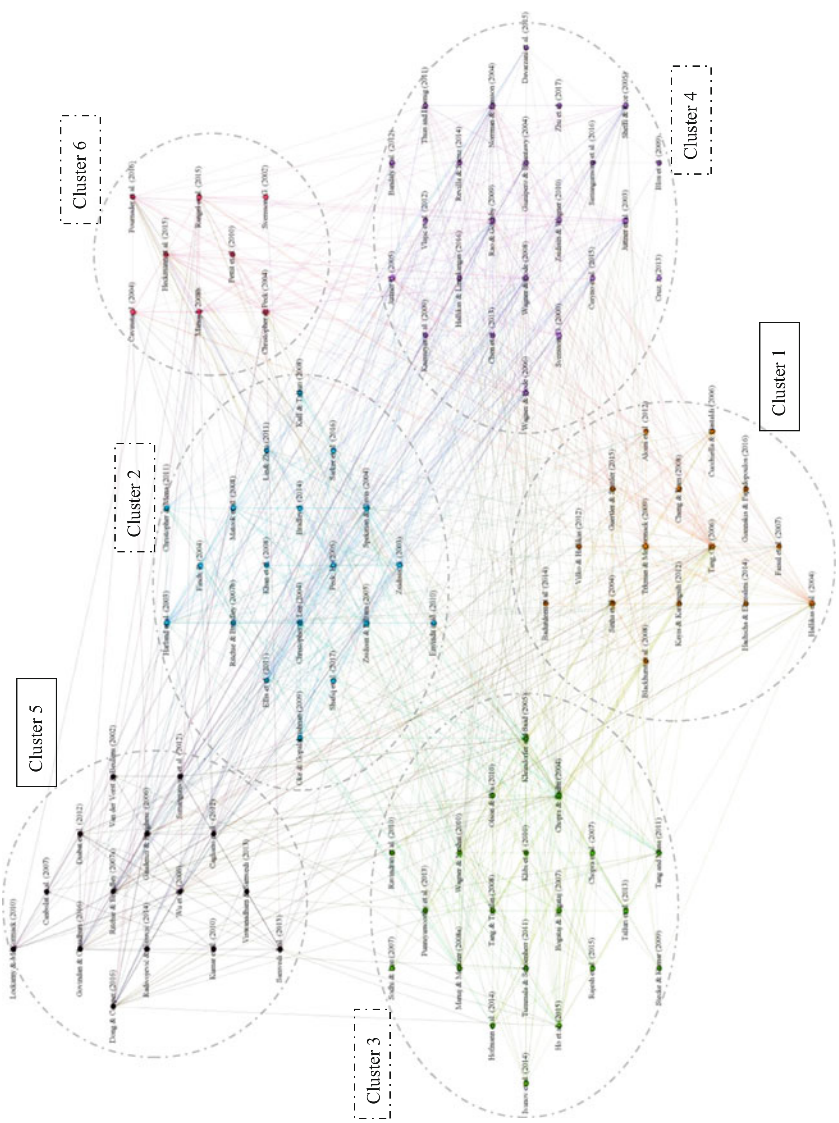


Fig. 5 Six clusters of researchers formed during the period 2000–2017

Table 5 Contribution of researcher community clusters

Community cluster	Frequency of studies at top 15 GCS	Frequency of studies at top 15 closeness centrality	Main path analysis	Clusters of risks
1	3	2	0	5
2	0	5	3	3
3	7	2	1	4
4	3	5	5	5
5	0	0	5	11
6	2	1	0	0

- The frequency of studies contributed by a researcher community cluster in the main path analysis (Fig. 4).
- The frequency a researcher community cluster contributed the maximum number of risk types to a risk cluster. At the left side of Table 6, it is included within the brackets the number of community cluster contributing the highest number of risk types to a risk cluster.

Cluster 1. This cluster is associated with competitiveness problems, strategic (same frequency as community cluster 5) and reputation issues, problems arising from the financial market and regulatory and bureaucratic issues. It contributes three studies in the top 15 of the highest GCS, and two studies in the top 15 of closeness centrality.

Cluster 2. This cluster is associated with SC inbound problems, relational problems and risks labelled as "other." It encompasses highest number of studies in the top 15 of closeness centrality (same frequency as community cluster 4).

Cluster 3. This cluster is associated with demand-side risks, infrastructural problems, capacity problems and the financial capacity problems of the firm. It contains the highest number of studies in the top 15 of GCS measure.

Cluster 4. This cluster is associated with risks that are internal to the firm, industrial problems, financial capacity issues (same frequency with community cluster 3) and problems arising externally from the supply chain. It encompasses the highest number of studies in the top 15 for closeness centrality (same frequency as community cluster 2). Furthermore, it entails the highest number of studies included in the main path analysis (same frequency as community cluster 5).

Cluster 5. This cluster contributes significantly at the formation of most of the risk clusters. Specifically, it offers the highest number of risk types to 11 risk clusters. These risks are associated with production flows, firm's core competence, demand (same frequency as community cluster 3), transportation, informational, problem-specific (same frequency as community cluster 4), strategic, customer-related problems, cultural, regulatory and bureaucratic, and global problems. Furthermore, it entails the highest number of studies included in the main path analysis (same frequency as community cluster 4).

Cluster 6. Despite the fact that this community cluster contributed two studies in the top 15 of GCS, and one study in the top 15 of closeness centrality, it cannot be characterized as an exemplar in terms of contributing to risk clusters.

The point here is that although the extent of contribution to supply chain risk categorization for each community of researchers differs, all the clusters contributed to the development of the topic.

4.4 How Can Consensus Be Achieved Across the Supply Chain Risk Classification Studies Published Since 2000? (RQ4)

This chapter revisited the topic of supply chain risk classification by exploring its historical development and offers a new inclusive typology by forming a level of among different clusters of researchers.

Our review indicates that numerous studies have impacted the development of the supply chain risk classification topic (Tables 2 and 3). Despite the merit of these studies, there is not a consensus among them because numerous classification criteria have been used as higher order constructs since 2000 (Table 4) and others do not include risk factors in the suggested classification scheme (Fig. 3). The most recent attempt comes from Rangel et al. (2015) who offer a supply chain risk classification based on the SCOR model which was formed using studies originating from peer-reviewed literature, conference papers and Ph.D. thesis. Our review indicates a much larger literature (up to 2017) that includes about 100 studies. Furthermore, milestone studies indicated by main path analysis (Fig. 4) offer clear-cut definitions, in addition to their other strengths, in comparison with other studies.

Therefore, to answer RQ4 we follow Rangel et al. (2015) by looking for a consensus about supply chain risk classification using broader criteria and a larger group of articles. We believe this will help the field's development.

To achieve that, we used as our starting point the risk clustering approach of Rangel et al. (2015) to classify risks according to the similarity of their definitions. At a second stage, for each cluster of risks formed, we reviewed risk-type definitions to achieve consensus among them (Rangel et al. 2015).

Table 6 depicts the result of the process to form clusters of risks according to definition similarity or according to risk factors. On the left side, the table depicts the name of the risk cluster while the number in brackets denotes which researcher community cluster contributed the maximum number of risk types. On the right side, the table depicts the different risk types found for each risk cluster, while the number in brackets denotes the frequency of appearance.

The typology of supply chain risks this study recommends; that is, the result of a level of consensus among different clusters of researchers (see Fig. 5) is divided into:

- Risks internal to the firm (Table 7),

Table 6 Types of risk clusters (adapted from Rangel et al. 2015)

Cluster of risks by definition similarity	Risk types		
Group 1: Production flow problems [5]	Disruptions [14] Delays [5] Natural [4] Production/manufacturing [8] Process/manufacturing [2]	Engineering/production capability and capacity [1] Production flexibility [1] Accidents [1] Hazard vulnerability [1]	Distortions [1] Availability [1] Disasters [1] Product characteristics [1] Physical risks [1]
Group 2: Competitiveness problems [1]	Competitiveness [9] Inertia [3] Innovational [1] Technological [5]	Resources [4] Lack of expertise [1] Macro [1] Product factors [1]	R&D uncertainty [1] Weaknesses in resources, development and flexibility [1]
Group 3: Core competence [5]	Process [11] Operational [6] Operations [8] Product [3]	Failure to deliver on time [1] Supply chain control mechanisms [1]	Sensitivity [1] Flexibility [1] Part-specific [1]
Group 4: Demand [3, 5]	Demand [34] Forecast [12] Wholesaler [1] Downstream [1]		
Group 5: SC Inbound problems [2]	Supply [54] Sustainability [3] Delivery failures [2] Cost failure [2] Economic [2]	Flexibility failure [1] General confidence failure [1] Operational [1] Quantity [1] Technology [1]	Management [1] Innovation capability [1] Raw materials [1] Upstream [1] Employee turnover [1]
Group 6: Transportation problems [5]	Transportation [8] Logistics [4] Lead time [4] Physical [1] On time delivery [1]	Transit time [1] Miss the target [1] Delivery service [1] Supply chain discontinuity [1]	Operational/technological [1] Shipment quantity increases [1]

(continued)

Table 6 (continued)

Cluster of risks by definition similarity	Risk types		
Group 7: Infrastructural [3]	Infrastructural [4] Security [3] Endogenous assets [1] Breakdown and hazard risks [1] Asset impairment risk [1]	Facilities [1] Deliberate threats [1]	
Group 8: Informational [5]	Informational [19] Security [3] System [3] Planning and control [1]		
Group 9: Capacity [3]	Capacity [7]		
Group 10: Problem-specific issues [4, 5]	Problem-specific [2] Decision complexity [2]		
Group 11: Strategic problems [1, 5]	Strategic [6] Management-related issues [1]		
Group 12: Customer-related problems [5]	Customer [6] Customer disruptions [1]		
Group 13: Organizational-related problems [4]	Organizational [15] Management [6] Labour instability [1] Internal legal issues [1]	Operating uncertainties [1] Credit [1]	
Group 14: Cultural [5]	Cultural/linguistic [6]		

(continued)

Table 6 (continued)

Cluster of risks by definition similarity	Risk types		
Group 15: Global Problems [5]	Sustainability risks [3] Inventory [12] Chain configuration [10] Network risk [3]	Quality [11] Control [2] Holistic sources of disturbance [1] Safety [1]	Interaction [1] Lack of coverage [1] Environmental [1]
Group 16: Decision-maker problems [None]	Decision maker [2] Individual attributes [1]		
Group 17: Industrial [4]	Market [7] Industry [4] Price fluctuations [4] Input market [2]	Product market [2] Stochastic cost [1]	
Group 18: Reputation [1]	Reputation [2] Financial/economic [1] Liability [2]		
Group 19: Financial capacity problems [3, 4]	Financial [4] Receivables [4] Credit uncertainties [1] Payment [1]		
Group 20: Financial market problems [1]	Exchange rate price [6] Economic [3] Financial [2] Procurement [4]	Macroeconomic [3] Oil price increase [1] Continuous [1] Fiscal risk [1]	Risks due to exchange rates, taxes and fuel prices [1]

(continued)

Table 6 (continued)

Cluster of risks by definition similarity	Risk types		
Group 21: Relationship problems [2]	Lack of ownership [2] Chaos [5] Behavioural [2] Intellectual Property [7]	Partner-specific [6] Relational [4] Dependence and opportunism [2] Lack of trust and opportunism [2] Dependence [2]	Connectivity [1] Outsourcing [1] Counterfeit [1] Switching time [1] Volume of business given [1] Nature of the source [1]
Group 22: Regulatory, Legal and Political [1, 5]	Customs regulations [2] Legal [6] Political [9] Policy [4] Regulatory [3]	Econo-political risks [1] Organizational [1] Terrorism and political instability [1] Miscellaneous [1]	Sociopolitical risks [1] Macroeconomic [1] Social [1] Technological elements of the operating environment (including legal and regulatory issues) [1]
Group 23: Lack of control over external environment [4]	Environmental [21] Catastrophic [6] Natural Hazards [4] Social [11]	Macroenvironment [3] External [5] Technical or implementation failure [1] Contextual [1]	Discrete [1] Turbulence [1] Value at risk [1] Accidents [1]
Group 24: Other [2]	Low [2] High [2] Intermediate [2] Very low [1]	Parallel interaction [2] Cost [2] Survival [1]	Tactical [1]

Table 7 Risks internal to the firm

Risk	Definition	Risk factors	Relevant references
Infrastructure	Arises from unwanted failures caused by intentional or unintentional acts associated with the infrastructure (e.g. IT, vehicles) maintained by a focal firm to execute internal or external supply chain operations	Unavailability of information with suppliers, IT breakdown, bugs/hackers, security of IT, incompatible IT systems, denial of service, equipment failure, vandalism at vehicles	Spekman and Davis (2004), Chopra and Sodhi (2004), Canbolat et al. (2008), Wagner and Bode (2008), Blackhurst et al. (2008), Manuj and Mentzer (2008a), Olson and Dash Wu (2010), Ho et al. (2015)
Strategic	Arises from unwanted events that can negatively affect the implementation of a focal firm's business strategy	Not effective change management, lack of knowledge of SCM benefits, outdated culture	Harland et al. (2003), Aloini et al. (2012)
Problem-specific	Arises from the complexity associated with the multiple dimensions of risk decision-making such as long-term planning, goals and constraints, and interrelationships among risks	Interrelationships among risks, long-term planning, goals and constraints	Rao and Goldsby (2009), Simangusong et al. (2012, 2016)

(continued)

Table 7 (continued)

Risk	Definition	Risk factors	Relevant references
Decision–maker-specific	Arises from individual or group level attributes within an organization	Bounded rationality, shortage of knowledge and experience, cognitive abilities	Rao and Goldsby (2009), Ellis et al. (2011)
Reputation	Arises from unwanted events that can impose a reputational damage to a focal firm	Poor product quality, late deliveries, dishonesty, patent infringement, price fixing accusations	Badurdeen et al. (2014), Giannakis and Papadopoulos (2016), Hallikas and Lintukangas (2016)
Capacity	It can arise either from the inflexibility of a focal firm to increase the level of capacity when required, or from capacity's overutilization/underutilization and can result in delays in the production process	Cost of capacity, capacity flexibility, overutilization of capacity, underutilization of capacity	Chopra and Sodhi (2004), Blackhurst et al. (2008), Tummala and Schoenherr (2011), Rajesh et al. (2015)
Financial capacity (receivables)	Arises from customers' financial difficulties that can result to delays or interruptions in the money flows towards a focal firm	Delayed payments from debtors, changes in the financial strength of customers, bankruptcy of customers, number of customers	Harland et al. (2003), Chopra and Sodhi (2004), Blackhurst et al. (2008), Ceryno et al. (2015), Rajesh et al. (2015)

- Risks internal to the supply chain (Table 8),
- Risks external to the supply chain (Table 9).

5 Conclusions

This chapter revisited the topic of supply chain risk categorization by exploring its historical development and offering a new inclusive typology by forming a level of among different clusters of researchers.

We found that about 26 studies were the most impactful on the topic of supply chain classification demonstrating the highest bibliometric measures (GCS, closeness centrality). Nevertheless, despite the growth of the studies on the topic in recent years, none of the existing typologies is complete, though most overlap. The formation of consensus among researchers on supply chain risk classifications has been fragmented, when considering over time the suggestion of classification schemes without risk factors and the use of different criteria to classify supply chain risks. By conducting a main path analysis, we identified the strengths of milestone studies that rely on the use of theory, the suggestion of clear-cut definitions and the use of quantitative approaches to categorize supply chain risk according to probability and impact. After identifying the different clusters of researcher communities and stating their contributions, we were motivated by the weaknesses of current classification schemes to develop an inclusive typology that is the result of a level of consensus among different researcher clusters. Accordingly, we used Rangel and colleagues' (2015) approach as a starting point to classify risk types into clusters by the similarity of their definitions. Next, for each risk cluster formed, we reviewed definitions of the risk-type demonstrating the highest frequency of appearance to achieve a consensus among multiple definitions.

To the best of the authors' knowledge, this is the first study that performs a systematic literature network analysis (SLNA) to review the topic of supply chain risk classification and achieves a level of consensus among researchers from about 100 studies. In this way, it leverages a substantially higher number of studies comparing to Rangel et al. (2015) to form a level of consensus. As a result, it contributes to the development of supply chain risk identification. This may accommodate the operationalization of supply chain risks in a way that makes sense to most researchers. From a managerial point of view, it offers an inclusive typology that is a result of state-of-the-art literature that may help decision-makers to better identify and understand supply chain risks.

Our findings are different from seminal studies on the same topic (e.g. Rao and Goldsby 2009) for the following reasons. First, we shed light on the historical development of the supply chain risk classification topic using an SLNA. This should help clarify the literature for future research efforts in supply chain risk identification while offering practitioners a further understanding of the development of supply chain risk typologies. Second, we developed an inclusive but parsimonious supply

Table 8 Risks internal to the supply chain

Risk	Definition	Risk factors	Relevant references
Supplier operational	It arises from unwanted events that may affect supplier output in terms of quality, quantity and cost which can result in unfulfilled or delayed orders to the focal firm	Quality problems, not anticipated quantity, not anticipated cost, significant variation in lead time, supplier delays, material availability, inappropriate technology	Van der Vorst and Beulens (2002), Zsidisin and Ellram (2003), Simangusong et al. (2012), Chen and Wu (2013), Shafiq et al. (2017)
Supplier economic	It arises from unwanted events that may harm a supplier's financial health and can lead to bankruptcy, insolvency or financial instability resulting to unfilled or delayed orders to the focal firm	Difficulties in making payments, financial instability, problems in cash flows, limited number of customers, shortage of raw materials, deteriorated reputation in the market	Wagner and Neshat (2010), Bradley (2014), Sarker et al. (2016), Shafiq et al. (2017)
Cultural	Arises from limited knowledge of cultural idiosyncrasies and language differences among supply chain partners that can result in delays or other failures	Language differences, limited knowledge of cultural differences	Canbolat et al. (2008), Manuj and Mentzer (2008b), Cagliano et al. (2012), Govindan and Chaudhuri (2016)
Relational	It arises from mistrust, lack of understanding, unnecessary interventions, second guessing among supply chain actors. Their effects are known as "chaos effects" driven by supply chain complexity	Mistrust, lack of understanding, second-guessing, supply chain complexity	Jüttner et al. (2003), Matook et al. (2009)
Demand	Arises from potential variations between forecasted and actual demand	Forecast errors, poor supply chain coordination, poor information sharing, long-term horizons, demand volatility, rationing and shortage rumours	Wagner and Bode (2006, 2008), Tummala and Schoenherr (2011), Chen and Wu (2013), Samvedi et al. (2013)

(continued)

Table 8 (continued)

Risk	Definition	Risk factors	Relevant references
Transportation	Arises from unwanted events associated with the delivery of raw materials or finished products that can impose delays in their movement	Port strikes, failures in the distribution network, carrier breakdown, failures in the distribution network, inaccessible information about shipment	Canbolat et al. (2008), Blackhurst et al. (2008), Tummala and Schoenherr (2011), Bradley (2014), Rajesh et al. (2015)
Inventory	It arises from excessive number of inventories and product value which can impose unnecessary holding costs or excessive product obsolescence	High inventory cost, product value, excessive amount of inventory, rate of product obsolescence	Chopra and Sodhi (2004), Blackhurst et al. (2008), Matook et al. (2009), Tummala and Schoenherr (2011), Rajesh et al. (2015)
Legal, bureaucratic and regulatory	Arises from litigations against the firm by stakeholders internal to the supply chain (e.g. suppliers, customers)	Litigations by internal to the supply chain stakeholders (e.g. suppliers, customers)	Harland et al. (2003), Wu et al. (2006), Radivojević and Gajović (2014)
Sustainability	Arises from ecological-, social- or ethical-related violations materializing during the execution of global operations by members of the chain (e.g. suppliers, distributors), leading to harmful reactions from external stakeholders (e.g. NGO) that may harm a focal firm	CO_2 emissions by chain partners, health and safety violations, child labour, the absence of water treatment, unnecessary packaging, low wages, not using ecologically friendly waste disposal	Christopher et al. (2011), Hofmann et al. (2014), Govindan and Chaudhuri (2016), Giannakis and Papadopoulos (2016), Sarker et al. (2016), Shafiq et al. (2017).
Financial capacity (receivables)	Arises from customers' financial difficulties that can result to delays or interruptions in the money flows towards a focal firm	Delayed payments from debtors, changes in the financial strength of customers, bankruptcy of customers, number of customers	Cavinato (2004); Chopra and Sodhi (2004), Blackhurst et al. (2008), Ceryno et al. (2015), Rajesh et al. (2015)
Consumer risk	Arises from a focal firm's inability to comply with customer preferences	Difficulties in order fulfilment, changes in customer preferences, delayed delivery, inappropriate quality	Hallikas et al. (2004), Hachicha and Elmsalmi (2014)

Table 9 Risks external to the supply chain

Risk	Definition	Risk factors	Relevant references
Competitiveness	Arises from changing market conditions associated with the entry of new competitors or rivalry among current ones, technology changes in product/process, which can result in the loss or reduction of a focal firm's competitive position	Rapid changes in product/process technology, lack of information about competitor	Cucchiela and Gastaldi (2006), Manuj and Mentzer (2008a), Badurdeen et al. (2014); Ceryno et al. (2015), Zhu et al. (2017)
Input market	It arises from the inability of a focal firm to acquire anticipated quantity or quality of inputs in the transformation process and can affect the competitiveness and profitability of a supply chain	Lack of alternative suppliers, inability to meet significant quantity increases, variability in quality of raw materials, unexpected raw material increases, scarcity of raw materials	Rao and Goldsby (2009), Matook et al. (2009), Vlajic et al. (2012), Ceryno et al. (2015)
Political risk	Arises from unwanted dramatic changes in the political system that can negatively affect a focal firm's ability to compete	Political turmoil, disturbances from counties interested in the focal firm's project, weak government, nationalization, trade tariffs increase, quota restriction, change in taxation	Harland et al. (2003), Wu et al. (2006), Canbolat et al. (2008), Badurdeen et al. (2014), Ceryno et al. (2015)
Catastrophic	It arises from high impact—low probability potential events associated with man-made deliberate acts (e.g. terrorism), unintentional man-made acts or natural hazards (e.g. hurricanes, earthquakes, tsunamis)	Terrorism, war, nuclear accidents, earthquakes, hurricanes, tsunamis, floods	Wagner and Bode (2008), Knemeyer et al. (2009), Stecke and Kumar (2009), Cagliano et al. 2012, Govindan and Chaudhuri (2016), Radivojević and Gajović (2014), Rajesh et al. (2015)
Financial market	Arises from changes associated with macroeconomic factors, especially exchange, inflation or interest rates and may ultimately lead to the increase of raw material prices	Changes in exchange rates, high rates of inflation, changes to interest rates	Chopra and Sodhi (2004), Canbolat et al. (2008), Blackhurst et al. (2008), Manuj and Mentzer (2008a, b), Cruz (2013), Rajesh et al. (2015)

chain risk typology which resolves at some extent overlaps and omissions in previous typologies.

6 Limitations of the Study

This research has two main limitations. First, HistCite from Clarivate Analytics did not report GCS measures or interrelationships with other nodes for specific studies of interest. This means results of Table 2 are hindered by the unavailability of data for some studies. A second limitation of this study is inter-rater reliability. Specifically, one rater was used which may have negatively affected the articulation of risk clusters or the achievement of consensus among risk types definitions for each cluster.

7 Recommendations for Future Research

Future research should move from typologies to taxonomies. The review indicates that while the literature offers numerous typologies, there is limited research devoted to developing taxonomies of supply chain risk. Therefore, we encourage researchers to develop taxonomies of supply chain risks by using empirical methods in multiple industries. This will move the field forward and may help firms to accommodate the identification of risks in their supply chain. Testing the supply chain risk typology offered in this chapter would be a solid step in developing taxonomies. Our last recommendation regards the more extensive use of managerial theories to inform the development of supply chain risk typologies/taxonomies. Only very few of the reviewed studies make use of theoretical lenses (e.g. Peck 2005). This lack of theory means that while the literature can offer many categorizations, it cannot explain why managers should categorize as such or how they should respond to risks if they materialize.

This chapter traces the historical development of the categorization component of supply chain risk identification. Categorization is a sub-component of supply chain risk identification, and when it is not done correctly, managers cannot manage the risks. Yet the literature has focused much more on managing the risks. Hopefully, the parsimonious but inclusive typology offered in this chapter will form the foundation of future research that rectifies that misalignment.

Acknowledgements We acknowledge the use of HistCite from Clarivate Analytics to identify studies of interest using GCS measure. We also acknowledge the use of Gephi to visually adjust citation networks that are free to use for commercial use (https://ephi.rg/egal/aq/). Last, we confirm that the first author has been granted permission to use Pajek (De Nooy et al. 2011) for academic purposes by Dr. Mvar (Andrej.Mrvar@fdv.uni-lj.si). This study was conducted while the first author Michalis Louis was a Doctoral Student in UCD Michael Smurfit Graduate Business School. This author received a Doctoral Scholarship from the school from 2015 to 2019.

References

Adhitya, A., Srinivasan, R., & Karimi, I. A. (2009). Supply chain risk identification using a HAZOP-based approach. *AIChE Journal, 55*(6), 1447–1463.

Aloini, D., Dulmin, R., Mininno, V., & Ponticelli, S. (2012). Supply chain management: A review of implementation risks in the construction industry. *Business Process Management Journal, 18*(5), 735–761.

Aqlan, F., & Lam, S. S. (2015). A fuzzy-based integrated framework for supply chain risk assessment. *International Journal of Production Economics, 161,* 54–63.

Aynaud, T., & Guillaume, J. L. (2010, May). Static community detection algorithms for evolving networks. In *2010 Proceedings of the 8th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt)* (pp. 513–519). IEEE.

Badurdeen, F., Shuaib, M., Wijekoon, K., Brown, A., Faulkner, W., Amundson, J., et al. (2014). Quantitative modeling and analysis of supply chain risks using Bayesian theory. *Journal of Manufacturing Technology Management, 25*(5), 631–654.

Bandaly, D., Satir, A., Kahyaoglu, Y., & Shanker, L. (2012). Supply chain risk management—I: Conceptualization, framework and planning process. *Risk Management, 14*(4), 249–271.

Blackhurst, J. V., Scheibe, K. P., & Johnson, D. J. (2008). Supplier risk assessment and monitoring for the automotive industry. *International Journal of Physical Distribution & Logistics Management, 38*(2), 143–165.

Blos, M. F., Quaddus, M., Wee, H. M., & Watanabe, K. (2009). Supply chain risk management (SCRM): A case study on the automotive and electronic industries in Brazil. *Supply Chain Management: An International Journal, 14*(4), 247–252.

Bogataj, D., & Bogataj, M. (2007). Measuring the supply chain risk and vulnerability in frequency space. *International Journal of Production Economics, 108*(1–2), 291–301.

Bradley, J. R. (2014). An improved method for managing catastrophic supply chain disruptions. *Business Horizons, 57*(4), 483–495.

Busse, C., Schleper, M. C., Weilenmann, J., & Wagner, S. M. (2017). Extending the supply chain visibility boundary: Utilizing stakeholders for identifying supply chain sustainability risks. *International Journal of Physical Distribution & Logistics Management, 47*(1), 18–40.

Cagliano, A. C., De Marco, A., Grimaldi, S., & Rafele, C. (2012). An integrated approach to supply chain risk analysis. *Journal of Risk Research, 15*(7), 817–840.

Canbolat, Y. B., Gupta, G., Matera, S., & Chelst, K. (2008). Analysing risk in sourcing design and manufacture of components and sub-systems to emerging markets. *International Journal of Production Research, 46*(18), 5145–5164.

Cavinato, J. L. (2004). Supply chain logistics risks: From the back room to the board room. *International Journal of Physical Distribution & Logistics Management, 34*(5), 383–387.

Ceryno, P. S., Scavarda, L. F., & Klingebiel, K. (2015). Supply chain risk: Empirical research in the automotive industry. *Journal of Risk Research, 18*(9), 1145–1164.

Chen, P. S., & Wu, M. T. (2013). A modified failure mode and effects analysis method for supplier selection problems in the supply chain risk environment: A case study. *Computers & Industrial Engineering, 66*(4), 634–642.

Chopra, S., Reinhardt, G., & Mohan, U. (2007). The importance of decoupling recurrent and disruption risks in a supply chain. *Naval Research Logistics (NRL), 54*(5), 544–555.

Chopra, S., & Sodhi, M. S. (2004). Managing risk to avoid supply-chain breakdown. *MIT Sloan Management Review, 46*(1), 53.

Christopher, M., & Lee, H. (2004). Mitigating supply chain risk through improved confidence. *International Journal of Physical Distribution & Logistics Management, 34*(5), 388–396.

Christopher, M., Mena, C., Khan, O., & Yurt, O. (2011). Approaches to managing global sourcing risk. *Supply Chain Management: An International Journal, 16*(2), 67–81.

Christopher, M., & Peck, H. (2004). Building the resilient supply chain. *The International Journal of Logistics Management, 15*(2), 1–14.

Colicchia, C., & Strozzi, F. (2012). Supply chain risk management: A new methodology for a systematic literature review. *Supply Chain Management: An International Journal, 17*(4), 403–418.
Costantino, N., & Pellegrino, R. (2010). Choosing between single and multiple sourcing based on supplier default risk: A real options approach. *Journal of Purchasing and Supply Management, 16*(1), 27–40.
Cruz, J. M. (2013). Mitigating global supply chain risks through corporate social responsibility. *International Journal of Production Research, 51*(13), 3995–4010.
Cucchiella, F., & Gastaldi, M. (2006). Risk management in supply chain: A real option approach. *Journal of Manufacturing Technology Management, 17*(6), 700–720.
Davarzani, H., Zanjirani Farahani, R., & Rahmandad, H. (2015). Understanding econo-political risks: Impact of sanctions on an automotive supply chain. *International Journal of Operations & Production Management, 35*(11), 1567–1591.
De Nooy, W., Mrvar, A., & Batagelj, V. (2011). *Exploratory social network analysis with Pajek* (Vol. 27). Cambridge: Cambridge University Press.
Denyer, D., & Tranfield, D. (2009). Producing a systematic review. In D. A. Buchanan & A. Bryman (Eds.), *The Sage handbook of organizational research methods* (pp. 671–689). London: Sage Publications.
Diabat, A., Govindan, K., & Panicker, V. V. (2012). Supply chain risk management and its mitigation in a food industry. *International Journal of Production Research, 50*(11), 3039–3050.
Dong, Q., & Cooper, O. (2016). An orders-of-magnitude AHP supply chain risk assessment framework. *International Journal of Production Economics, 182,* 144–156.
Ellis, S. C., Shockley, J., & Henry, R. M. (2011). Making sense of supply disruption risk research: A conceptual framework grounded in enactment theory. *Journal of Supply Chain Management, 47*(2), 65–96.
Enyinda, C. I., Mbah, C. H., & Ogbuehi, A. (2010). An empirical analysis of risk mitigation in the pharmaceutical industry supply chain: A developing-country perspective. *Thunderbird International Business Review, 52*(1), 45–54.
Faisal, M. N., Banwet, D. K., & Shankar, R. (2007, January). Management of risk in supply chains: SCOR approach and analytic network process. *Supply Chain Forum: An International Journal, 8*(2), 66–79.
Fan, Y., & Stevenson, M. (2018a). A review of supply chain risk management: Definition, theory, and research agenda. *International Journal of Physical Distribution & Logistics Management, 48*(3), 205–230.
Fan, Y., & Stevenson, M. (2018b). Reading on and between the lines: Risk identification in collaborative and adversarial buyer–supplier relationships. *Supply Chain Management: An International Journal, 23*(4), 351–376.
Finch, P. (2004). Supply chain risk management. *Supply Chain Management: An International Journal, 9*(2), 183–196.
Fischhoff, B., Watson, S. R., & Hope, C. (1984). Defining risk. *Policy Sciences, 17*(2), 123–139.
Gaudenzi, B., & Borghesi, A. (2006). Managing risks in the supply chain using the AHP method. *The International Journal of Logistics Management, 17*(1), 114–136.
Giannakis, M., & Papadopoulos, T. (2016). Supply chain sustainability: A risk management approach. *International Journal of Production Economics, 171,* 455–470.
Giunipero, L. C., & Aly Eltantawy, R. (2004). Securing the upstream supply chain: A risk management approach. *International Journal of Physical Distribution & Logistics Management, 34*(9), 698–713.
Govindan, K., & Chaudhuri, A. (2016). Interrelationships of risks faced by third party logistics service providers: A DEMATEL based approach. *Transportation Research Part E: Logistics and Transportation Review, 90,* 177–195.
Guertler, B., & Spinler, S. (2015). Supply risk interrelationships and the derivation of key supply risk indicators. *Technological Forecasting and Social Change, 92,* 224–236.
Hachicha, W., & Elmsalmi, M. (2014). An integrated approach based-structural modeling for risk prioritization in supply network management. *Journal of Risk Research, 17*(10), 1301–1324.

Hallikas, J., Karvonen, I., Pulkkinen, U., Virolainen, V. M., & Tuominen, M. (2004). Risk management processes in supplier networks. *International Journal of Production Economics, 90*(1), 47–58.

Hallikas, J., & Lintukangas, K. (2016). Purchasing and supply: An investigation of risk management performance. *International Journal of Production Economics, 171,* 487–494.

Harland, C., Brenchley, R., & Walker, H. (2003). Risk in supply networks. *Journal of Purchasing and Supply Management, 9*(2), 51–62.

Heckmann, I., Comes, T., & Nickel, S. (2015). A critical review on supply chain risk—Definition, measure and modeling. *Omega, 52,* 119–132.

Hendricks, K. B., & Singhal, V. R. (2003). The effect of supply chain glitches on shareholder wealth. *Journal of operations Management, 21*(5), 501–522.

Hendricks, K. B., & Singhal, V. R. (2005a). An empirical analysis of the effect of supply chain disruptions on long-run stock price performance and equity risk of the firm. *Production and Operations Management, 14*(1), 35–52.

Hendricks, K. B., & Singhal, V. R. (2005b). Association between supply chain glitches and operating performance. *Management Science, 51*(5), 695–711.

Ho, W., Zheng, T., Yildiz, H., & Talluri, S. (2015). Supply chain risk management: A literature review. *International Journal of Production Research, 53*(16), 5031–5069.

Hofmann, H., Busse, C., Bode, C., & Henke, M. (2014). Sustainability-related supply chain risks: Conceptualization and management. *Business Strategy and the Environment, 23*(3), 160–172.

Ivanov, D., Sokolov, B., & Dolgui, A. (2014). The Ripple effect in supply chains: Trade-off ‘efficiency-flexibility-resilience’ in disruption management. *International Journal of Production Research, 52*(7), 2154–2172.

Jüttner, U. (2005). Supply chain risk management: Understanding the business requirements from a practitioner perspective. *The International Journal of Logistics Management, 16*(1), 120–141.

Jüttner, U., Peck, H., & Christopher, M. (2003). Supply chain risk management: Outlining an agenda for future research. *International Journal of Logistics: Research and Applications, 6*(4), 197–210.

Kayis, B., & Dana Karningsih, P. (2012). SCRIS: A knowledge-based system tool for assisting manufacturing organizations in identifying supply chain risks. *Journal of Manufacturing Technology Management, 23*(7), 834–852.

Keow Cheng, S., & Hon Kam, B. (2008). A conceptual framework for analysing risk in supply networks. *Journal of Enterprise Information Management, 21*(4), 345–360.

Kern, D., Moser, R., Hartmann, E., & Moder, M. (2012). Supply risk management: Model development and empirical analysis. *International Journal of Physical Distribution & Logistics Management, 42*(1), 60–82.

Khan, O., Christopher, M., & Burnes, B. (2008). The impact of product design on supply chain risk: A case study. *International Journal of Physical Distribution & Logistics Management, 38*(5), 412–432.

Kleindorfer, P. R., & Saad, G. H. (2005). Managing disruption risks in supply chains. *Production and operations management, 14*(1), 53–68.

Klibi, W., Martel, A., & Guitouni, A. (2010). The design of robust value-creating supply chain networks: A critical review. *European Journal of Operational Research, 203*(2), 283–293.

Knemeyer, A. M., Zinn, W., & Eroglu, C. (2009). Proactive planning for catastrophic events in supply chains. *Journal of Operations Management, 27*(2), 141–153.

Kull, T. J., & Talluri, S. (2008). A supply risk reduction model using integrated multicriteria decision making. *IEEE Transactions on Engineering Management, 55*(3), 409–419.

Kumar, S. K., Tiwari, M. K., & Babiceanu, R. F. (2010). Minimisation of supply chain cost with embedded risk using computational intelligence approaches. *International Journal of Production Research, 48*(13), 3717–3739.

Lavastre, O., Gunasekaran, A., & Spalanzani, A. (2014). Effect of firm characteristics, supplier relationships and techniques used on supply chain risk management (SCRM): An empirical investigation on French industrial firms. *International Journal of Production Research, 52*(11), 3381–3403.

Light, R. J., & Pillemer, D. B. (1984). *Summing up: The science of reviewing research*. Cambridge, MA: Harvard University Press.

Lin, Y., & Zhou, L. (2011). The impacts of product design changes on supply chain risk: A case study. *International Journal of Physical Distribution & Logistics Management, 41*(2), 162–186.

Liu, J. S., & Lu, L. Y. (2012). An integrated approach for main path analysis: Development of the Hirsch index as an example. *Journal of the Association for Information Science and Technology, 63*(3), 528–542.

Lockamy, A., III, & McCormack, K. (2010). Analysing risks in supply networks to facilitate outsourcing decisions. *International Journal of Production Research, 48*(2), 593–611.

Manuj, I., & Mentzer, J. T. (2008a). Global supply chain risk management. *Journal of Business Logistics, 29*(1), 133–155.

Manuj, I., & Mentzer, J. T. (2008b). Global supply chain risk management strategies. *International Journal of Physical Distribution & Logistics Management*, *38*(3), 192–223.

March, J. G., & Shapira, Z. (1987). Managerial perspectives on risk and risk taking. *Management Science, 33*(11), 1404–1418.

Matook, S., Lasch, R., & Tamaschke, R. (2009). Supplier development with benchmarking as part of a comprehensive supplier risk management framework. *International Journal of Operations & Production Management, 29*(3), 241–267.

Mitchell, V. W. (1995). Organizational risk perception and reduction: A literature review. *British Journal of Management, 6*(2), 115–133.

Mrvar, A., & Batagelj, V. (2018). Programs for analysis and visualization of very large networks reference manual. Retrieved from http://rvar2.dv.i/ajek%0/ajekman.df.

Neiger, D., Rotaru, K., & Churilov, L. (2009). Supply chain risk identification with value-focused process engineering. *Journal of operations Management, 27*(2), 154–168.

Norrman, A., & Jansson, U. (2004). Ericsson's proactive supply chain risk management approach after a serious sub-supplier accident. *International Journal of Physical Distribution & Logistics Management, 34*(5), 434–456.

Oke, A., & Gopalakrishnan, M. (2009). Managing disruptions in supply chains: A case study of a retail supply chain. *International Journal of Production Economics, 118*(1), 168–174.

Olson, D. L., & Dash Wu, D. (2010). A review of enterprise risk management in supply chain. *Kybernetes*, *39*(5), 694–706.

Peck, H. (2005). Drivers of supply chain vulnerability: An integrated framework. *International Journal of Physical Distribution & Logistics Management, 35*(4), 210–232.

Pettit, T. J., Fiksel, J., & Croxton, K. L. (2010). Ensuring supply chain resilience: Development of a conceptual framework. *Journal of Business Logistics, 31*(1), 1–21.

Pournader, M., Rotaru, K., Kach, A. P., & Razavi Hajiagha, S. H. (2016). An analytical model for system-wide and tier-specific assessment of resilience to supply chain risks. *Supply Chain Management: An International Journal, 21*(5), 589–609.

Punniyamoorthy, M., Thamaraiselvan, N., & Manikandan, L. (2013). Assessment of supply chain risk: Scale development and validation. *Benchmarking: An International Journal*, *20*(1), 79–105.

Radivojević, G., & Gajović, V. (2014). Supply chain risk modeling by AHP and Fuzzy AHP methods. *Journal of Risk Research, 17*(3), 337–352.

Raj Sinha, P., Whitman, L. E., & Malzahn, D. (2004). Methodology to mitigate supplier risk in an aerospace supply chain. *Supply Chain Management: An International Journal, 9*(2), 154–168.

Rajesh, R., Ravi, V., & Venkata Rao, R. (2015). Selection of risk mitigation strategy in electronic supply chains using grey theory and digraph-matrix approaches. *International Journal of Production Research, 53*(1), 238–257.

Rangel, D. A., de Oliveira, T. K., & Leite, M. S. A. (2015). Supply chain risk classification: Discussion and proposal. *International Journal of Production Research, 53*(22), 6868–6887.

Rao, S., & Goldsby, T. J. (2009). Supply chain risks: A review and typology. *The International Journal of Logistics Management, 20*(1), 97–123.

Ravindran, A. R., Ufuk Bilsel, R., Wadhwa, V., & Yang, T. (2010). Risk adjusted multicriteria supplier selection models with applications. *International Journal of Production Research, 48*(2), 405–424.

Revilla, E., & Sáenz, M. J. (2014). Supply chain disruption management: Global convergence vs national specificity. *Journal of Business Research, 67*(6), 1123–1135.

Ritchie, B., & Brindley, C. (2007a). Supply chain risk management and performance: A guiding framework for future development. *International Journal of Operations & Production Management, 27*(3), 303–322.

Ritchie, B., & Brindley, C. (2007b). An emergent framework for supply chain risk management and performance measurement. *Journal of the Operational Research Society, 58*(11), 1398–1411.

Ritchie, B., & Marshall, D. V. (1993). *Business risk management*. London: Chapman & Hall.

Samvedi, A., Jain, V., & Chan, F. T. (2013). Quantifying risks in a supply chain through integration of fuzzy AHP and fuzzy TOPSIS. *International Journal of Production Research, 51*(8), 2433–2442.

Sarker, S., Engwall, M., Trucco, P., & Feldmann, A. (2016). Internal visibility of external supplier risks and the dynamics of risk management silos. *IEEE Transactions on Engineering Management, 63*(4), 451–461.

Shafiq, A., Johnson, P. F., Klassen, R. D., & Awaysheh, A. (2017). Exploring the implications of supply risk on sustainability performance. *International Journal of Operations & Production Management, 37*(10), 1386–1407.

Sheffi, Y., & Rice, J. B., Jr. (2005). A supply chain view of the resilient enterprise. *MIT Sloan Management Review, 47*(1), 41.

Simangunsong, E., Hendry, L. C., & Stevenson, M. (2012). Supply-chain uncertainty: A review and theoretical foundation for future research. *International Journal of Production Research, 50*(16), 4493–4523.

Simangunsong, E., Hendry, L. C., & Stevenson, M. (2016). Managing supply chain uncertainty with emerging ethical issues. *International Journal of Operations & Production Management, 36*(10), 1272–1307.

Småros, J., Lehtonen, J. M., Appelqvist, P., & Holmström, J. (2003). The impact of increasing demand visibility on production and inventory control efficiency. *International Journal of Physical Distribution & Logistics Management, 33*(4), 336–354.

Sodhi, M. S., & Lee, S. (2007). An analysis of sources of risk in the consumer electronics industry. *Journal of the Operational Research Society, 58*(11), 1430–1439.

Sodhi, M. S., Son, B. G., & Tang, C. S. (2012). Researchers' perspectives on supply chain risk management. *Production and Operations Management, 21*(1), 1–13.

Spekman, R. E., & Davis, E. W. (2004). Risky business: Expanding the discussion on risk and the extended enterprise. *International Journal of Physical Distribution & Logistics Management, 34*(5), 414–433.

Stecke, K. E., & Kumar, S. (2009). Sources of supply chain disruptions, factors that breed vulnerability, and mitigating strategies. *Journal of Marketing Channels, 16*(3), 193–226.

Svensson, G. (2000). A conceptual framework for the analysis of vulnerability in supply chains. *International Journal of Physical Distribution & Logistics Management, 30*(9), 731–750.

Svensson, G. (2002). A typology of vulnerability scenarios towards suppliers and customers in supply chains based upon perceived time and relationship dependencies. *International Journal of Physical Distribution & Logistics Management, 32*(3), 168–187.

Talluri, S. S., Kull, T. J., Yildiz, H., & Yoon, J. (2013). Assessing the efficiency of risk mitigation strategies in supply chains. *Journal of Business Logistics, 34*(4), 253–269.

Tang, C. S. (2006). Perspectives in supply chain risk management. *International Journal of Production Economics, 103*(2), 451–488.

Tang, O., & Musa, S. N. (2011). Identifying risk issues and research advancements in supply chain risk management. *International Journal of Production Economics, 133*(1), 25–34.

Tang, C., & Tomlin, B. (2008). The power of flexibility for mitigating supply chain risks. *International Journal of Production Economics, 116*(1), 12–27.

Thun, J. H., & Hoenig, D. (2011). An empirical analysis of supply chain risk management in the German automotive industry. *International Journal of Production Economics, 131*(1), 242–249.

Trkman, P., & McCormack, K. (2009). Supply chain risk in turbulent environments—A conceptual model for managing supply chain network risk. *International Journal of Production Economics, 119*(2), 247–258.

Tummala, R., & Schoenherr, T. (2011). Assessing and managing risks using the supply chain risk management process (SCRMP). *Supply Chain Management: An International Journal, 16*(6), 474–483.

Van der Vorst, J. G., & Beulens, A. J. (2002). Identifying sources of uncertainty to generate supply chain redesign strategies. *International Journal of Physical Distribution & Logistics Management, 32*(6), 409–430.

Vilko, J. P., & Hallikas, J. M. (2012). Risk assessment in multimodal supply chains. *International Journal of Production Economics, 140*(2), 586–595.

Viswanadham, N., & Samvedi, A. (2013). Supplier selection based on supply chain ecosystem, performance and risk criteria. *International Journal of Production Research, 51*(21), 6484–6498.

Vlajic, J. V., Van der Vorst, J. G., & Haijema, R. (2012). A framework for designing robust food supply chains. *International Journal of Production Economics, 137*(1), 176–189.

Wagner, S. M., & Bode, C. (2006). An empirical investigation into supply chain vulnerability. *Journal of Purchasing and Supply Management, 12*(6), 301–312.

Wagner, S. M., & Bode, C. (2008). An empirical examination of supply chain performance along several dimensions of risk. *Journal of Business Logistics, 29*(1), 307–325.

Wagner, S. M., & Neshat, N. (2010). Assessing the vulnerability of supply chains using graph theory. *International Journal of Production Economics, 126*(1), 121–129.

Wu, T., Blackhurst, J., & Chidambaram, V. (2006). A model for inbound supply risk analysis. *Computers in Industry, 57*(4), 350–365.

Xiao, T., & Yang, D. (2008). Price and service competition of supply chains with risk-averse retailers under demand uncertainty. *International Journal of Production Economics, 114*(1), 187–200.

Zhu, Q., Krikke, H., & Caniëls, M. C. (2017). Integrated supply chain risk management: A systematic review. *The International Journal of Logistics Management, 28*(4), 1123–1141.

Zsidisin, G. A. (2003a). Managerial perceptions of supply risk. *Journal of Supply Chain Management, 39*(2), 15–27.

Zsidisin, G. A. (2003b). A grounded definition of supply risk. *Journal of Purchasing and Supply Management, 9*(5–6), 217–224.

Zsidisin, G. A., & Ellram, L. M. (2003). An agency theory investigation of supply risk m anagement. *Journal of Supply Chain Management, 39*(2), 15–27.

Zsidisin, G. A., Ellram, L. M., Carter, J. R., & Cavinato, J. L. (2004). An analysis of supply risk assessment techniques. *International Journal of Physical Distribution & Logistics Management, 34*(5), 397–413.

Zsidisin, G. A., Panelli, A., & Upton, R. (2000). Purchasing organization involvement in risk assessments, contingency plans, and risk management: An exploratory study. *Supply Chain Management: An International Journal, 5*(4), 187–198.

Zsidisin, G. A., Melnyk, S. A., & Ragatz, G. L. (2005). An institutional theory perspective of business continuity planning for purchasing and supply management. *International Journal of Production Research, 43*(16), 3401–3420.

Zsidisin, G. A., Petkova, B., Saunders, L. W., & Bisseling, M. (2016). Identifying and managing supply quality risk. *The International Journal of Logistics Management, 27*(3), 908–930.

Zsidisin, G. A., & Wagner, S. M. (2010). Do perceptions become reality? The moderating role of supply chain resiliency on disruption occurrence. *Journal of Business Logistics, 31*(2), 1–20.

Chapter 21
The Impact of Supply Chain Disruptions on Organizational Performance: A Literature Review

Mahour M. Parast and Mansoor Shekarian

1 Introduction

The management of disruption risks in a supply chain has received increasing attention in the last decade due to widespread recognition that all supply chains are susceptible to a variety of disruptions that can have both immediate and long-term effects on the supply chain (Nooraie and Parast 2015; Aqlan and Lam 2015; Chen et al. 2013; Ho et al. 2015; Gligor et al. 2015; Purvis et al. 2014). Supply chain risk management remains a key managerial challenge that affects the performance of organizations. It is defined as "the identification of potential sources of risk and implementation of appropriate strategies through a coordinated approach among supply chain risk members, to reduce supply chain vulnerability" (Jüttner et al. 2003, p. 201). According to Kamalahmadi and Parast (2016), SCRM is concerned with the assessment of sources of risk across the supply chain and the development of strategies or capabilities to make organizations more responsive to supply chain disruptions.

Supply chain disruptions have been described as the occurrence of unpredictable and undesirable events such as natural disasters, loss of partnership relationships, and changes in customer preferences which undermine supply chain performance (Mandal 2014; Wagner and Bode 2008; Zsidisin et al. 2005; Zsidisin and Ellram 2003). These are some events that illustrate the negative consequences of disruptions on organizational performance: hurricane Harvey in Houston in 2017, hurricane Sandy in New York in 2012, the Indian Ocean tsunami in 2004, the Fukushima Daiichi nuclear disaster in Japan in 2011, the fire at a Philips plant in New Mexico in 2000 (which disrupted the supply chains of Nokia and Ericsson, leading to a

M. M. Parast (✉) · M. Shekarian
North Carolina A&T State University, Greensboro, NC, USA
e-mail: mahour@ncat.edu

M. Shekarian
e-mail: mshekarian@aggies.ncat.edu

G. A. Zsidisin and M. Henke (eds.), *Revisiting Supply Chain Risk*, Springer Series in Supply Chain Management 7, https://doi.org/10.1007/978-3-030-03813-7_21

financial loss in Ericsson of 400 million Euros), and an earthquake in Taiwan in 1999 that caused a supply shortage of DRAM chips, costing Apple many customer orders. Therefore, managing disruption risks in a supply chain has become a topic of paramount interest for both scholars and practitioners (Nooraie and Parast 2016; Kamalahmadi and Parast 2015; Gligor et al. 2015; Zsidisin and Wagner 2010; Tang and Tomlin 2008; Kleindorfer and Saad 2005; Zsidisin and Ellram 2003).

The impact of supply chain disruptions on firm performance has been recognized (Hendricks and Singhal 2005). However, some firms still do not invest in disruption mitigation strategies and do not develop capabilities to be more resilient to disruptions; their managers are not fully convinced that the benefits from improved responses to supply chain disruptions outweigh the costs of investing in supply chain disruption mitigation capabilities (Tang 2006; Chopra and Sodhi 2004). We aim to provide more clarity on the effect of supply chain disruptions on organizational performance.

In this chapter, we review the existing literature in SCRM and examine the effect of supply chain disruptions on organizational performance. We start by reviewing different theorizations and conceptualizations of SCRM. We later review the mitigation strategies (organizational capabilities) that firms can develop to reduce the negative effect of supply chain disruptions on organizational performance.

2 Conceptualization of Supply Chain Risk Management

Supply chain disruptions can be categorized in many different ways by using different perspectives, such as a corporate governance viewpoint, a financial risk viewpoint, or even in terms of a multi-level complex system (Peck 2004). Ho et al. (2015) divided supply chain risks into two categories: macro-risks and micro-risks. This same conceptualization is also referred to as catastrophic and operational (Sodhi et al. 2012) or disruption and operational (Tang 2006). Macro-risks refer to adverse, relatively rare external events or situations that might have a negative impact on organizational performance. This type of risk consists of natural risks (such as earthquakes and weather-related disasters) and man-made risks (such as war, terrorism, and political instability). In contrast, micro-risks refer to recurrent events originating directly from a company's internal activities and/or from relationships with partners in the supply chain. In addition, micro-risks can be divided into four subcategories: demand risk, manufacturing risk, supply risk, and infrastructural risk. Generally, macro-risks have much greater negative impact on companies compared to micro-risks (Ho et al. 2015).

Christopher and Peck (2004) provide another conceptualization of SCRM. Figure 1 shows the classification of supply chain risk by Christopher and Peck (2004). They suggested that there are three categories of disruption risk: (1) internal to the firm (process risk and control risk), (2) external to the firm and internal to the supply chain network (demand risk and supply risk), and (3) external to the network

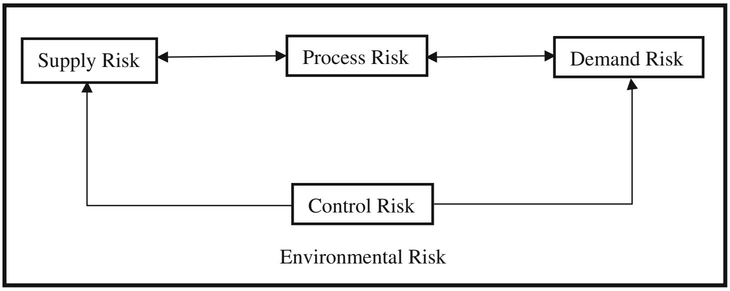


Fig. 1 Sources of risk in a supply chain (Christopher and Peck 2004)

(environmental risk). Thus, as depicted in Fig. 1, their framework proposes five different dimensions for disruption risk.

In their classification, process risks are the sequences of value-adding and managerial activities undertaken by the firm; control risks are the assumptions, rules, systems, and procedures that govern how an organization exerts control over the processes; demand risks relate to potential disturbances to the flow of products and information between the focal firm and the market; supply risks relate to potential disturbances to the flow of products or information emanating from within the network, upstream of the focal firm; and environmental risks can affect upstream, downstream or the focal firm, and any nodes or links in a supply chain.

Another categorization of supply chain risks is to separate them into operational risks and disruption risks (Chen et al. 2013). Disruption risks typically are about unplanned events with negative effects on a supply chain system; the events may be a result of man-made or natural disasters such as economic downturns, technology changes, terrorist attacks, hurricanes, or strikes. Operational risks are more about supply–demand coordination risks, which may result from inadequate or failed processes, control, people, or systems.

The Supply Chain Risk Leadership Council (SCRLC 2011) divides risks into two major categories: internal and external disruption risks. According to the SCRLC, external risks would further be grouped into end-to-end risks, supplier risks, and distribution risks. End-to-end risks include natural disasters, accidents, sabotage, terrorism, political uncertainty, labor unavailability, market challenges, lawsuits, and technological trends. Supplier risks include physical and regulatory systems, production problems, financial losses and premiums, and upstream supply risks. Distribution risks include infrastructure unavailability, lack of capacity, labor unavailability, cargo damage or theft, warehouse inadequacies, IT system inadequacies or failure, and multi-party supply pipelines. Some of the internal risks are operational problems, political uncertainty, demand variability, personnel availability, design uncertainty, planning failures, financial uncertainty, facility unavailability, testing unavailability, enterprise underperformance, and supplier relationship management (Aluda 2015).

3 Research Methodology

We use a systematic literature review approach to review the articles in SCRM between 2000 and 2017. This research approach has been used in previous studies in supply chain risk and resilience management (Kamalahmadi and Parast 2016; Ghadge et al. 2012; Tang and Musa 2010). We adapt their procedure using the two steps given below in order to examine our research questions pertaining to the relationship between supply chain disruption risks and organizational performance.

Step 1. Search databases and journals.
Step 2. Track references of publications obtained in Step 1.

In line with Kamalahmadi and Parast (2016), in the first step, we use the widely accepted quality rating published by the Association of Business Schools (ABS), UK, as Academic Journal Guide (AJG) 2017 for journals in three different domains of management: Operations Management/Supply Chain Management (OM/SCM), Operation Research and Management Science (OR/MS), and General Management (GM). A number of major databases, such as *Science Direct*, *Taylor and Francis*, *Google Scholar*, and *Emerald*, along with top journals in OM/SCM, OR/MS, and GM are used to identify published articles in supply chain disruption risks. The search keywords are based on terminologies that are popular in SCRM literature, such as "supply chain resilience," "organizational performance," "resiliency in supply chain," along with "disruption," "risk," or "uncertainty."

To assess the effect of supply chain disruptions on organizational performance, we used the risk classification mentioned in Sect. 2 (Fig. 1), proposed by Christopher and Peck (2004), to identify articles that clearly refer to specific source of supply chain disruption risks. We used this classification because (1) it is the most widely cited article in SCRM, and (2) it makes a clear distinction between different supply chain disruption risks.

In order to ensure that all the related articles are included in the research, in each research paper we studied, we tracked the references in order to further identify relevant studies being cited by the authors (Step 2). This procedure resulted in identifying 50 quality research publications that are the basis of the literature review presented in this study.

4 The Effect of Supply Chain Disruptions on Supply Chain Performance

In this section, we review the existing literature in SCRM, and then discuss research findings that relate supply chain disruption management to organizational performance.

A supply chain is described as a chain linking each element from customer and supplier through manufacturing and services so that the flow of material, money, and information can be effectively managed to meet the business requirements (Stevens 1989). The impact of supply chain disruptions on organizational performance can be attributed to increased complexity of the supply chain and instability in global supply chains. Some severe negative economic consequences of supply chain disruptions on firm's performance have been extensively documented in both academic and practitioner literature (Nyamah et al. 2017; Hendricks and Singhal 2005). Therefore, the ability of an organization to respond to external threats and to mitigate disruption across the supply chain is directly related to the firm's short-term and long-term performance (Nyamah et al. 2017; Kilubi 2016; Hendricks and Singhal 2003; Sheffi 2005; Chopra and Sodhi 2004).

The performance of supply chain needs to be assessed across the organizations in order to ensure global optimization along the supply chain channels (Sundram et al. 2016). Currently, most companies realize that in order to create an efficient supply chain, supply chain management needs to be assessed for its performance (Thun and Hoenig 2011; Hendricks and Singhal 2005; Gunasekaran et al. 2001). According to an empirical study by Johnson and Templar (2011) in the manufacturing firms in the UK, improved supply chain performance leads to improved firm performance. Revilla and Saenz (2017) suggested that best-performance firms should pursue the adoption of an integral SCRM strategy that goes beyond operational processes and spans the firm's relationships with buyers and suppliers. In addition, Ritchie and Brindley (2007) suggested that performance and risk are interconnected and require deliberate and robust implementation of supplier management tools and controls to maximize performance while controlling the consequential risks. Christopher and Towill (2001) explained the issues related to market qualifier and market winner in a supply chain; they identified cost, quality, lead time, and service level as four performance measures for supply chains. In addition, Agarwal et al. (2006) considered market sensitiveness, information drivers, process integration, and flexibility as supply chain performance dimensions. Furthermore, Hendricks and Singhal (2003) presented a set of operational measures that relate supply chain performance to areas such as forecasting and planning accuracy, supplier performance, delivery performance, lead time, inventory, capacity, and quality. Although the choice and importance of operational measures will vary across firms, the performance of a firm on its chosen operational metrics will determine the efficiency, reliability, and responsiveness of its supply chains.

4.1 The Effect of Demand Disruption Risk on Supply Chain Performance

Chopra and Sodhi (2014) asserted that supply chain disruptions negatively affect financial performance of the firms. They suggested two strategies for reducing supply chain fragility through containment while simultaneously improving financial performance: (1) segmenting the supply chain and (2) regionalizing the supply chain.

In addition, high demand uncertainty also requires centralizing to achieve reasonable levels of performance.

4.2 The Effect of Supply Disruption Risk on Supply Chain Performance

Schoenherr (2010) examines the relationship between purchase risk and purchase performance within an outsourcing context. The results indicated that the link between purchase risk and performance was not statistically significant. Therefore, the level of risk in an outsourcing relationship apparently does not influence performance. Based on the results of an empirical study by Zsidisin and Ellram (2003), reducing the likelihood of supply risk occurrence can result in improved supplier performance. For example, when suppliers incorporate the latest technological advances in their operations, and adhere to specified quality standards, the cost of doing business with that supplier is significantly reduced. The total costs of suppliers due to delivery failures, inspection costs, product returns, and warranties are significantly reduced. Transaction costs are lowered in the exchange, resulting in overall improved supply chain performance in the dyad between purchasing firms and suppliers. Another empirical study by Zsidisin et al. (2004) suggests that supply risk assessments involve a proactive approach by purchasing organizations for understanding the impact and likelihood that detrimental events can have on inbound supply. This provides firms with insight for best managing the risk. In addition, they found that supply risk assessment may also occur as a secondary benefit of the implementation of the proactive supply management tools, particularly those that focus on addressing supplier quality issues, improving supplier performance, and preventing supply interruptions.

4.3 The Effect of Environmental Disruption Risk on Supply Chain Performance

In a systematic literature review by Zhu et al. (2017), they suggested that customer service, operational, and financial performance are dominant performance dimensions in an integrated SCRM context. They identified three sources of environmental risks: legal risks, infrastructural risks, and catastrophic risks. As disruptions originating from infrastructural and catastrophic risks always happen suddenly, joint decision-making (i.e., operational integration) helps the supply chain quickly react to such disruptions. In this sense, short-term performance metrics (i.e., customer service, operational, and financial performance) are more suitable for assessment. In contrast, legal changes have a long-term impact on the focal firm and its supply chain. Hence, long-term relational integration and strategic information integration are more helpful for legal risk mitigation. To evaluate their outcomes, long-term-oriented performance metrics (i.e., innovation and market performance) are recommended.

4.4 The Effect of Control Disruption Risk on Supply Chain Performance

In turbulent environments, it is important for supply chain partners to collaborate to enhance supply chain performance. Using the data collected from 350 manufacturing firms in China, Li et al. (2015) indicated that the effectiveness of risk information sharing and risk-sharing mechanisms in improving financial performance can be strengthened by collaborative relationship characteristics such as relationship length, supplier trust, and shared supply chain risk management understanding. Their results showed that both information-sharing and risk-sharing mechanisms improve financial performance. In addition, managers should employ a supply chain management perspective for managing supply chain risks, and they should pay attention to collaborate with supply chain partners to work jointly to mitigate supply chain risks. They specifically advocated two joint supply chain risk management practices, risk information sharing and risk-sharing mechanisms, to enhance collaboration with suppliers. Risk information sharing is an essential element supporting supply chain risk management information systems that manage the critical, proprietary risk-related information in the supply chain. Without such systems, the implementation of many modern supply chain risk management practices would not be possible. Risk-sharing mechanisms are concerned with formal arrangements (e.g., contracts) for supply chain partners' shared obligations and responsibilities toward SCRM. This practice reduces supply chain risk-related disputes between supply chain members and provides them with specific guidelines on how they should work together to mitigate supply chain risks.

In addition, they offered guidelines indicating that these two joint SCRM practices are particularly effective when certain relationship characteristics exist. Specifically, risk information sharing is particularly effective when there is a high level of long-term orientation or supplier trust, whereas risk-sharing mechanisms are particularly effective when a high level of shared supply chain risk management understanding exists between the firms. Such practice guidelines help firms decide if their supply chain relationships are favorable for them to implement these joint supply chain risk management practices.

4.5 General Studies in Supply Chain Risk Management

Supply chain disruptions can have long-term negative effects on a firm's financial performance. For instance, Hendricks and Singhal (2005) investigated the long-term stock price effects and equity risk effects of disruptions based on a sample of 827 disruption announcements made over a 10-year period. They found that companies suffering from supply chain disruptions experience 33–40% lower stock returns relative to their industry benchmarks over a 3-year time period that starts 1 year before and ends 2 years after the disruption announcement date. In another study, Bode et al. (2011) asserted that supply chain disruption may have direct and indirect negative effects on a firm's performance objectives. However, the mentioned studies were focused on supply chain disruption risks in a very general way, and they did not identify specific types of disruption (e.g., demand, process, or supply); thus, it would be difficult to examine the impact of a specific type of supply chain disruption on organizational performance.

4.6 Comparing the Effect of Different Sources of Risks on Supply Chain Performance

Chopra and Sodhi (2004) asserted that receivable risks, inventory risks, and capacity risks would have a negative impact on financial performance. Using data from top-level executives in logistics and supply chain management in Germany, Wagner and Bode (2008) found that there are negative associations between supply- and demand-side risks and supply chain performance. However, in terms of some sources of environmental risks such as regulatory, legal, and bureaucratic risks, infrastructure risks, and catastrophic risks, their study did not provide any empirical evidence for a negative relationship with supply chain performance. They showed that the frequency of occurrence of severe disruptions has substantial negative consequences on the health of the affected firms. Given that severe sources of environmental risks that lead to the release of ad hoc announcements occur less frequently than "everyday" demand-side and supply-side disruptions, these latter risk sources are in fact very important for achieving high performance in a supply chain. Thus, decision-makers should focus on demand-side and supply-side disruptions as sources of risk.

In an empirical study of the agri-food industry, Nyamah et al. (2017) showed that demand, supply, weather, logistics/infrastructure, and financial risk sources significantly undermined the firm's performance, while risks emerging from biological/environmental, management/operational, policy/regulations, and political-related issues do not have a significant impact on the performance of the agri-food supply chain in Ghana. Their results showed that risks account for about half of the overall agri-food chain performance in Ghana. In addition, to achieve a better performance, managers need to employ adequate and efficient forecasting systems to mitigate the demand- and supply-related risks to avoid disruptions of the three main flows (i.e., material, financial, and information) of the chain.

Chen et al. (2013) investigated the impact of supply chain risks on supply chain performance by administering a survey questionnaire. Their study showed that while demand risk and process risk have a significant impact on supply chain performance, supply risk was not found to have a direct relationship with supply chain performance. On the other hand, there is a very strong relationship between supply risk and process risk; therefore, one explanation of this unsupported relationship is that the negative effect of supply risk on supply chain performance is fully mediated by process risk. By considering the material requirement planning (MRP) system as an example to demonstrate this effect; if there is a possible delay in the material supply, the buying firm may mitigate this risk by planning a delivery window into MRP or make changes in production plans between periods. This eliminates the direct impact of delayed incoming material but induces possible variations into the production process.

In contrast to supply risk, which has no direct effect on supply chain performance, their findings illustrated that demand risk has a direct negative effect on operational performance. This may suggest that firms find it more difficult to cope with demand variations than supply variations, which makes a negative effect from the demand side more visible. There are two plausible explanations here. First, operational performance is concerned with finished products, while supply risks are concerned with raw materials or components. The problem with supplied materials does not directly affect the end product since it can be rectified within the production system. Second, in conjunction with the inventory issue, the direct effect of demand risk on performance could suggest that firms feel more reluctant to keep the inventory of finished products to counter demand fluctuations compared with keeping a stock of raw materials to counter supply risks.

More interestingly, their results revealed that process risk has the strongest direct effect on supply chain performance, but supply risk and demand risk equally affect the performance significantly (while there is no direct effect of supply risk on supply chain performance, their results showed that its total effect through process risk on supply chain performance is the same as the direct effect of demand risk on supply chain performance).

All in all, their study provided important results for supply chain managers. They concluded that while managing supply chain partners (i.e., suppliers and customers) is increasingly important, managers must not lose track of the internal processes of the firm. Their research showed that process risk has the strongest direct effect on supply chain performance, and more importantly, the majority of external risks on either the supply side or demand side are mediated through process risk. So, it should be imperative for companies to build responsive and robust production processes to respond to any external changes and minimize the effect of those changes on supply chain performance.

Using a two-stage mixed-integer model, Kamalahmadi and Parast (2017) showed the significant impact of two phenomena on supply chain performance: (1) environmental disruption and (2) supplier dependence. They examined how the selection and allocation of warehouses, backup suppliers, and protected suppliers are affected when very reliable/unreliable suppliers, very reliable/unreliable regions, and very dependent/independent suppliers exist. In addition, their results showed that operations and supply chain managers may need to work with a different set of suppliers when disruptions happen; the selection and resource allocation of suppliers are quite different when disruption dependence and environmental risk are incorporated into the model.

Thus, failing to address all types of disruptions and suppliers' interdependence in the design of a supply chain and the development of disruption mitigation strategies could have significant negative consequences on firm performance. They suggested that the importance of environmental risk should be stressed more by managers, since the firm has less control over environmental risk compared to other sources of risk in the supply chain. Their findings also show the importance of regionalization in mitigating supply chain disruptions.

Using resource dependency theory, Paulraj and Chen (2007) examined the direct effect of supply chain environmental uncertainties on strategic supply management. Their study showed that strategic supply chain management can lead to collaborative advantage and ultimately create a "win-win" situation for the supplier and buyer firms. Their findings indicated that under conditions of technology uncertainty, firms can choose to strengthen coordination between supply partners by recognizing and embracing the idea of resource dependence. Such a collective action can help firms acquire and apply additional knowledge toward overcoming the adverse effect of technology and product obsolescence. In addition, under conditions of significant supply uncertainties, the negative behavioral patterns of the suppliers can be avoided by the introduction of comprehensive interfirm coordination and relationship-specific assets. Furthermore, the significant impact of supplier performance on buyer performance and the significant indirect effect of strategic supply management on buyer performance through supplier performance also suggest that when supplier performance is improved, the buying firm also stands to benefit. Therefore, collaborative partners need to share a common vision of the future and have an understanding that they can both achieve sustainable advantage by pursuing strategic initiatives that are mutually beneficial.

Thun and Hoenig (2011) argued that supply chain performance can be improved by mitigating supply chain disruption risks through implementing reactive and preventive instruments. Preventive instruments are cause-related measurements that strive to lower the probability of risk occurrence, while reactive instruments are effect-oriented measurements that strive for mitigating the negative impact of an incident. In their study, the group using preventive instruments for SCRM had higher average values in terms of increased flexibility and decreased stocks. Furthermore, this group had higher values concerning reactivity and cost reduction. In contrast, the group representing companies with reactive SCRM had higher average values in terms of a reduction of the bullwhip effect and greater resilience to external disruptions.

Additionally, their study revealed that SCRM has the potential to improve supply chain performance in the automotive industry. They showed that those companies having a low implementation degree of SCRM instruments had lower average values in all of the investigated performance criteria such as resilience against external disruptions, improvement in reactivity, and flexibility. Furthermore, reactive instruments of SCRM are less implemented than preventive instruments. A reason for this might be the fact that reactive instruments are cost-intensive, since they are primarily based on resource-binding redundancies such as safety stock.

In a further step, the study grouped companies by a cluster analysis, separating the companies into groups pursuing reactive or preventive SCRM; their results are

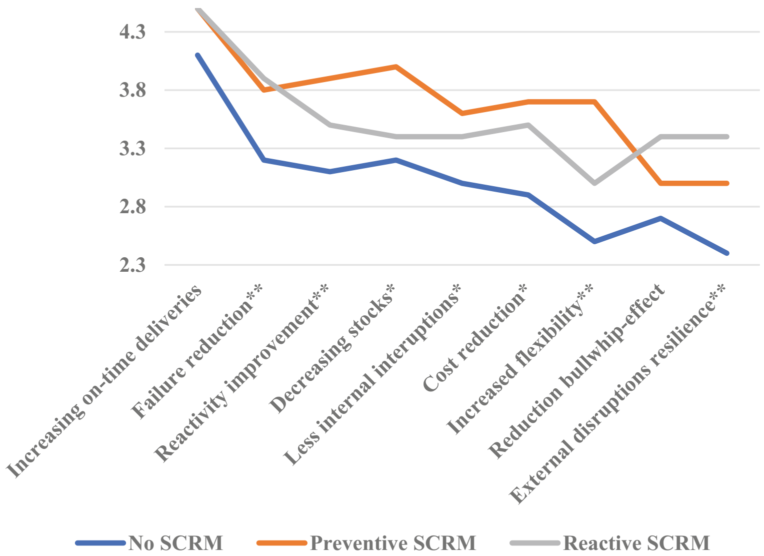


Fig. 2 Supply chain performance measures (Thun and Hoenig 2011)

presented in Fig. 2. The group using preventive instruments shows higher values in terms of increased flexibility, decreased stocks, increased reactivity, and cost reduction. The group using reactive instruments shows higher average values concerning a reduction of the bullwhip effect and increased resilience to external disruptions. These results showed that reactive supply chain management is effective in terms of external impacts but leads to inefficiencies due to the redundancies. In contrast, preventive SCRM supports the creation of a resilient supply chain.

Quang and Hara (2017) proposed a conceptual model, which represents relationships among risks and supply chain performance (Fig. 3). In the center of the model there are three core risks pertaining to the product flow: (1) operational risk, (2) supply risk, and (3) demand risk. These three risks have a direct effect on supply chain performance, which is measured by five crucial dimensions including supplier performance, internal business, innovation and learning, customer service, and finance. According to the results of the structural equation model, the risk of operations, supply, and demand, respectively, have a detrimental effect on supply chain performance than in the competitive model because the push effect of other risks makes them more dangerous, resulting in increased impact on supply chain performance. In addition, through the push effect, the proposed risk can explain 73% variance of supply chain performance compared with 55% of the competitive model as supply chain performance is not only influenced by supply chain risks, but also by other factors, e.g., innovation and supply chain management practices. Therefore, if a firm can manage the mechanism of the push effect, they can mitigate the effect of disruption risks on supply chain performance.

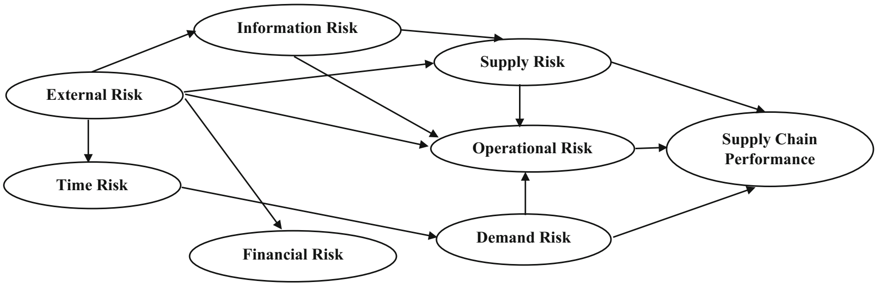


Fig. 3 Relationship among disruption risks and supply chain performance (Quang and Hara 2017)

5 Supply Chain Disruption Risk Management: Major Themes

5.1 Conceptualizations of Supply Chain Risk Management

Our review of the literature in SCRM suggests that SCRM has been conceptualized differently by different scholars. For instance, Jüttner et al. (2003) suggest four elements of managing supply chain risk: (1) assessing the risk sources, (2) identification of risk concepts, (3) tracking the risk drivers, (4) mitigation of risks. In addition, Kleindorfer and Saad (2005) identify three process elements: (1) specifying sources of risks and vulnerabilities, (2) assessments, and (3) mitigation. Furthermore, Sodhi et al. (2012) suggest four key elements for managing supply chain risks: (1) risk identification, to identify sources of risk and uncertainty, an initial step recommended by many researchers; (2) risk assessment, a process involving the evaluation of the likelihood and the impact of each source of risk; (3) risk mitigation, to reduce the likelihood of a particular risk's occurrence, reduce its potential impact, or both; and (4) responsiveness to risk incidents, to develop a response to each actual risk event so as to reduce its potential impact and hasten recovery. Event responses can be divided into responses to (1) operational risk events and (2) catastrophic risk events.

Using different conceptualizations and theorizations for SCRM has advanced our understanding of SCRM principles and premises, but it has also created confusion in terms of assessment of the validity of the results. Since researchers have used different frameworks and conceptualizations for SCRM, the results of their findings have not been easily comparable across different studies. We attempted to resolve this issue by reviewing the articles that have clearly defined the types of disruption they examined in their study.

5.2 Impact of Supply Chain Disruptions on Organizational Performance

According to our review of the literature, we found that environmental risks have been mentioned frequently in the literature as the important factor that has a negative impact on supply chain performance. Our review showed that studies emphasized different types of risk for their negative impact on supply chain performance: 42% of the studies emphasized supply risk, 25% emphasized environmental risk, 17% emphasized demand risk, 8% emphasized control risk, and 8% emphasized process risk. For instance, Wagner and Bode (2008) showed that supply-side and demand-side disruptions are more important than environmental disruptions for achieving high supply chain performance of German firms. Chen et al. (2013) indicated that process risk has the strongest direct effect on performance, and the majority of demand or supply risk is mediated through process risk. Li et al. (2015), using data collected from 350 manufacturing firms in China, found that the effectiveness of risk information sharing and risk-sharing mechanisms in improving financial performance can be strengthened by collaborative relationship characteristics such as relationship length, supplier trust, and shared supply chain risk management understanding.

Blackman et al. (2013) indicated that there is a diversity of approaches and different frameworks to measure the performance of supply chains, taking into account financial and non-financial measurements, operational performance, strategic performance, and high-level measures of overall firm performance such as profitability. Our review found that these measures are very important to evaluate supply chain performance during disruptions: delivery time, failure rate, process improvement rate, stocks level, internal interruption rate, cost, flexibility level, bullwhip effect rate, and external disruption rate (Thun and Hoenig 2011). However, there are some other important measures of performance such as service levels, lead time, quality measures, return on investments, and sales growth that have not been investigated in the literature (Viswanadham 2018; Quang et al. 2016; Viswanadham and Samvedi 2013; Merschmann and Thonemann 2011; Christopher and Towill 2001).

Future studies should examine the relationship between supply chain disruption risk management and organizational performance across different regions and multiple countries, taking into account the contextual and organizational variables that may positively or negatively moderate the relationship between disruption and performance. In addition, by conducting studies in different contexts, we would be able to advance theory development in the field through enhancing the external validity of the findings, and to ensure that our understanding of supply risk management practices and premises are valid in different contexts and regions, thereby improving the generalizability of the theory.

This completes our review of the impact of supply chain disruption risks on organizational performance. The next section provides an overview of the resiliency enhancers (i.e., organizational capabilities) that firms can develop for use in responding to disruptions.

6 Supply Chain Resiliency Enhancers

Supply chain resilience is concerned with reducing the impact of disruptions by identifying organizational capabilities (supply chain resiliency enhancers) that allow a supply chain to respond and recover at least to its original functional state (Zsidisin et al. 2016; Zsidisin and Wagner 2010; Sheffi 2005; Christopher and Peck 2004). There are several studies in the literature that emphasize the essential role of flexibility, agility, collaboration, and redundancy in creating supply chain resilience (Jain et al. 2017; Christopher and Peck 2004; Tukamuhabwa et al. 2015; Yang et al. 2017; Swafford et al. 2008; Tomlin 2006; Jüttner and Maklan 2011; Zsidisin and Wagner 2010). Flexibility refers to the ability of a firm to respond to long-term or fundamental changes in the supply chain and market environment by adjusting the configuration of the supply chain (Li et al. 2009; Blome et al. 2014). Agility can be described as the ability of a firm to efficiently change operating states in response to environmental uncertainty or volatile market conditions (Lim et al. 2017; Narasimhan et al. 2006). Supply chain collaboration refers to the ability of the firm to work efficiently with other entities for mutual benefits in areas such as forecasting, postponement, and risk sharing (Pettit et al. 2013). Redundancy involves the strategic and selective use of spare capacity and inventory that can be invoked to respond to a crisis, such as demand surges or supply shortages (Christopher and Peck 2004).

Shekarian and Parast (2018) investigated the impact of four dominant strategies of supply chain resiliency (flexibility, agility, collaboration, and redundancy) on mitigating supply chain disruptions. They found that the most important strategies in mitigating supply chain disruptions were, in order of importance: supply chain flexibility, collaboration, agility, and redundancy. They showed that more than 40% of the literature emphasized the crucial role of flexibility in enhancing supply chain resilience.

Merschmann and Thonemann (2011) found that firms matching their supply chain flexibility with the level of environmental uncertainty achieved higher firm performance than firms that failed to achieve this match. In addition, their results showed that the uncertainty of the environment should play an important role when deciding about the optimal degree of supply chain flexibility. The companies in their surveys that matched supply chain flexibility and environmental uncertainty achieved a performance of 4.1 (on a 5-point scale), while companies with a mismatch only achieved a performance of 3.1. Thus, the effort in matching supply chain flexibility to environmental uncertainty seems worthwhile.

Sanchez and Perez (2005) indicated that flexibility capabilities are enhanced in supply chains with higher environmental uncertainty, technological complexity, and mutual understanding, but with lower interdependence among the agents involved in the supply chain. Their research found that there is a positive relation between superior performance in flexibility capabilities and firm performance. However, the type of flexibility is important. Their results showed that firms enhance the basic flexibility capabilities (at the shop floor level) more than aggregate flexibility capa-

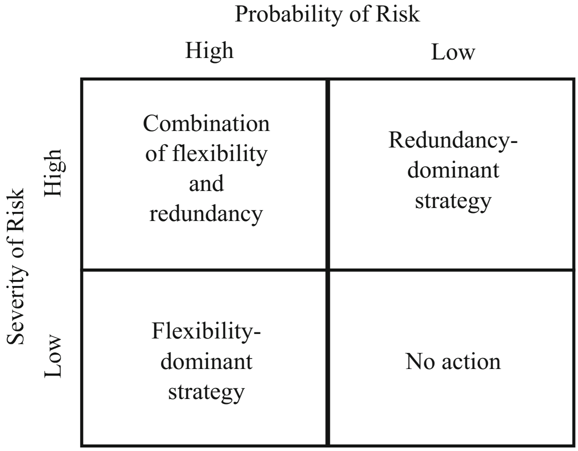


Fig. 4 Matching supply chain risk mitigation strategies with risk dimensions (Chang et al. 2015)

bilities (at the customer–supplier level). Aggregate flexibility capabilities are more positively related to firm performance than basic flexibility capabilities.

According to Chang et al. (2015), their conceptual framework presented in Fig. 4 proposes that no single strategic approach is optimal for all contexts of risks. Rather, focusing on redundancy (in high-severity/low-probability risk contexts) or flexibility (in low-severity/high-probability risk contexts), a combination of both (in high-severity/high-probability risk contexts), or doing nothing (in low-severity/low-probability risk contexts) may be the most effective approach to achieve better firm performance.

Li and Chan (2012) found that the performance of a collaborative transportation management supply chain is better than a supply chain without collaborative transportation management. Their results indicated that collaborative transportation management can significantly reduce costs and improve flexibility of companies in handling demand disruption problems. They concluded that collaborative transportation management is an efficient mechanism to handle demand disruption.

Patel et al. (2012) found that firms increase manufacturing flexibility in the presence of environmental uncertainty, and the firms with greater capabilities for manufacturing flexibility achieve higher performance. In addition, both operational absorptive capacity and operational ambidexterity moderate the relationship between environmental uncertainty and manufacturing flexibility and also moderate the relationship between manufacturing flexibility and firm performance. Also, absorptive capacity affects a firm's ability to implement time-based manufacturing practices. They indicated firms that are better able to acquire, assimilate, and transform information are more likely to respond to environmental uncertainty with manufacturing flexibility. Finally, they emphasized that ambidexterity enhances the likelihood that firms operating in uncertain environments will respond with flexible strategies.

Kilubi (2016) presented a SCRM framework to make a distinction between the ante-disruption and the post-disruption state, and between the proactive and reactive

Supply-side risks	Demand-side risks: low	Demand-side risks: high
	Ante disruption state	Post disruption state
low	**Supply chain type IV** **Proactive Strategy Approach** Visibility and Transparency, Partnerships/ Relationships	**Supply chain type I** **Reactive Strategy Approach** Postponement, Visibility and Transparency, Redundancy (Inventory), Multiple Sourcing and Flexible Contracts, Collaboration, Flexibility
high	**Supply chain type III** **Proactive Strategy Approach** Joint Planning and Coordination, Redundancy (Inventory), Visibility and Transparency	**Supply chain type II** **Reactive Strategy Approach** Flexibility, Postponement, Visibility and Transparency, Multiple Sourcing and Flexible Contracts, Redundancy (Inventory), Collaboration

Fig. 5 Supply chain risk management framework (Kilubi 2016)

strategy approach considering two supply chain attributes, namely supply-side risks and demand-side risks (Fig. 5). They asserted that reactive SCRM implies taking actions after an incident has occurred, while proactive SCRM means arranging ahead to alleviate hazards before they arise.

He indicated that organizations that setup supply chain type I with a reactive strategy approach follow the goal of reacting flexibly to demand fluctuations, mirroring an adequate level of price and service awareness. A supply chain type I beholds the demand-side attribute as possessing high levels of risk exposure during low levels of risk exposure for the supply-side attribute. In supply chain type II, both supply-side and demand-side risks are highly unstable, since supply chain type II regularly undergoes a change in which the customer requests are constantly unsteady, and many suppliers are undependable and restricted. Therefore, such companies put emphasis on their assets and capacities, quality, delivery reliability, and after-sales service. Consequently, organizations with an associated agile supply chain strategy consider both supply chain attributes (demand-side and supply-side risks) as possessing high levels of risk exposure. Contrariwise, a company that goes for the supply chain type III is highly exposed to supply-side risks, but little to demand-side risks. Thus, companies that apply a proactive strategy approach within supply chain type III usually hedge themselves against supplier uncertainty. Supply chains type IV are typically characterized by constant and foreseeable demand, lengthy product life cycle, and lesser net revenues. In this manner, organizations with a related efficient supply chain require a lower degree of responsiveness to prompt design feature changes and demand fluctuations.

7 Supply Chain Resiliency Enhancers: Major Findings

7.1 Flexibility

Flexibility improves supply chain resilience by enhancing adaptability during turbulent times (Fang et al. 2012; Christopher and Holweg 2011; Das 2011). This strategy demonstrates the flexibility of a firm in responding to environmental changes, demand changes, supply changes, and technology changes (Overby et al. 2006; Li et al. 2009; Dominik et al. 2015; Blome et al. 2014).

Supply chain flexibility is the most frequently mentioned strategy in the literature for mitigating supply chain disruptions (Shekarian and Parast 2018). The authors indicated that 40% of the reviewed studies showed that supply chain flexibility is the most important strategy in mitigating supply chain disruptions. In addition, the literature shows the impact of different types of supply chain flexibility on improving supply chain resilience (Das and Lashkari 2015; Tukamuhabwa et al. 2015; Tang and Tomlin 2008; Sheffi 2005; Christopher and Peck 2004). According to Shekarian and Parast (2018), manufacturing flexibility, supplier flexibility, process flexibility, and operational flexibility are the most important types of flexibility in coping with demand, supply, process, control, and environmental disruptions, respectively.

Future studies can examine the relative importance of different types of supply chain flexibility on improving a firm's resilience to supply chain disruptions. For example, Stevenson and Spring (2007) identified 21 dimensions of supply chain flexibility. Using the proposed framework by Christopher and Peck (2004), one avenue for future research is to examine the effect of different types of flexibility on mitigating different types of supply chain disruptions (i.e., demand, supply, environmental, control, and process risks) as depicted by Christopher and Peck (2004). By understanding these relationships, managers would be able to invest in the appropriate flexibility dimension to improve supply chain resilience.

7.2 Agility

Agility is described as the ability to efficiently change operating states as a response to environmental uncertainty or volatile market conditions (Lim et al. 2017; Narasimhan et al. 2006; Faisal et al. 2006). By reviewing the literature, we noticed that agility is one of the most powerful strategies for achieving a resilient supply chain, because it measures the capability to make rapid responses to changing conditions (Tukamuhabwa et al. 2015; Christopher and Peck 2004). Also, designing for agility is a risk management strategy that enables a firm to respond rapidly to market changes and potential or actual disruptions in the supply chain (Braunscheidel and Suresh 2009; Chopra and Sodhi 2004).

There are several types of supply chain agility: logistics agility, technology agility, relationship agility, and process agility (Ismail and Sharifi 2006). Future studies can examine the relative importance of these types of supply chain agility for improving a firm's resilience to supply chain disruptions. In addition, the impact of each type of supply chain agility on improving a supply chain's resilience to each of the five sources of risk proposed by Christopher and Peck (2004) has not yet been examined. By understanding these relationships, managers can better decide to invest in each type of supply chain agility to improve supply chain resilience.

7.3 Collaboration

Collaboration plays an important role in enhancing the competitive advantage of a supply chain and can significantly reduce overall cost and uncertainty (Gold et al. 2010; Carter and Rogers 2008). Besides, a high level of collaboration across a supply chain can help mitigate disruptions (Jain et al. 2017; Li et al. 2015; Chen et al. 2013). A higher degree of dependence on supply chain partners calls for a greater need for collaboration to supply chain disruptions (Revilla and Saenz 2017; Bode et al. 2011). Beske and Seuring (2014) asserted that collaboration can significantly reduce overall cost and uncertainty. Two major dimensions of collaboration in a supply chain are decision synchronization and incentive alignment; both are essential for successfully responding to disruptions in the supply chain (Jain et al. 2017).

Future studies can examine the relative importance of different dimensions of supply chain collaboration on improving a firm's resilience to supply chain disruptions. For example, Simatupang and Sridharan (2005) identified three dimensions for supply chain collaboration: information sharing, decision synchronization, and incentive alignment. However, the impact of each type of supply chain collaboration on enhancing the supply chain's resilience to each of the five sources of risk proposed by Christopher and Peck (2004) has not yet been examined. By understanding these relationships, managers can better invest in each dimension of supply chain collaboration to improve supply chain resilience.

7.4 Redundancy

According to Christopher and Peck (2004), redundancy involves the strategic and selective use of spare capacity and inventory that can be invoked during a crisis such as a demand surge or a supply shortage in either demand or supply. Sheffi and Rice

(2005) recommended that in order to create resiliency and enhance recovery from disruptions, building redundancy is an effective option. Kamalahmadi and Parast (2017) showed how implementation of three types of redundancy strategies (inventory, backup suppliers, and protected suppliers) can improve a firm's performance in a turbulent business environment where the firm needs to mitigate supply chain disruptions.

Future studies can examine the relative importance of different types of supply chain redundancy on improving a firm's resilience to supply chain disruptions. For example, Kamalahmadi and Parast (2017) and Chopra and Sodhi (2004) identified six types of supply chain redundancy strategies. However, the impact of each type of these strategies on improving a firm's response to different supply chain disruptions has not been examined in the literature. By understanding these relationships, managers can make an informed decision regarding investment in the appropriate redundancy strategy to improve supply chain resilience.

8 Conclusion

In this chapter, we addressed two research questions in SCRM. First, we examined the effect of supply chain disruptions on organizational performance. We then identified organizational capabilities (resilience enhancers) that improve an organization's response to supply chain disruptions. In reviewing the literature on SCRM, our focus was to relate the effect of different types of supply chain disruptions on organizational performance.

Our review of the literature suggests that while process disruption has the most negative effect on supply chain performance, supply disruption risk and demand disruption risk also affect organizational performance. Future studies should examine the relationship between supply chain disruptions and organizational performance with respect to many organizational and contextual factors in order to develop a more nuanced understanding of the relationship between disruptions and performance.

To cope with supply chain disruptions, firms need to invest in the supply chain capabilities identified as resilience enhancers. In that regard, improving supply chain flexibility is critical to achieve a higher level of organizational resilience, which enhances a firm's response to process disruptions. For supply chains that are exposed to demand risk, supply risk, and environmental risk, the best strategy is investing in supply chain flexibility. Organizations would be able to reduce the negative effect of control disruptions through investment in collaboration with their supply chain partners.

Acknowledgements This research is based upon work supported by the National Science Foundation (NSF) under Grant number 123887 (Research Initiation Award: Understanding Risks and Disruptions in Supply Chains and their Effect on Firm and Supply Chain Performance).

References

Agarwal, A., Shankar, R., & Tiwari, M. K. (2006). Modeling the metrics of lean, agile and leagile supply chain: An ANP-based approach. *European Journal of Operational Research, 173,* 211–225.

Aluda, K. M. (2015). *Supply chain risk management practices among telecommunications equipment vendors in Kenya: A case study of Nokia Kenya*. School of business: University of Nairobi.

Aqlan, F., & Lam, S. S. (2015). Supply chain risk modelling and mitigation. *International Journal of Production Research, 53*(18), 5640–5656.

Beske, P., & Seuring, S. (2014). Putting sustainability into supply chain management. *Supply Chain Management: An International Journal, 19*(3), 322–331.

Blackman, I. D., Holland, C. P., & Westcott, T. (2013). Motorola's global financial supply chain strategy. *Supply Chain Management: An International Journal, 18*(2), 132–147.

Blome, C., Schoenherr, T., & Eckstein, D. (2014). The impact of knowledge transfer and complexity on supply chain flexibility: A knowledge-based view. *International Journal of Production Economics, 147,* 307–316.

Bode, C., Wagner, S. M., Petersen, K. J., & Ellram, L. M. (2011). Understanding responses to supply chain disruptions: Insights from information processing and resource dependence perspectives. *Academy of Management Journal, 54*(4), 833–856.

Braunscheidel, M. J., & Suresh, N. C. (2009). The organizational antecedents of a firm's supply chain agility for risk mitigation and response. *Journal of Operations Management, 27,* 119–140.

Carter, C. R., & Rogers, D. S. (2008). A framework of sustainable supply chain management: Moving toward new theory. *International Journal of Physical Distribution and Logistics Management, 38*(5), 360–387.

Chang, W., Ellinger, A. E., & Blackhurst, J. (2015). A contextual approach to supply chain risk mitigation. *The International Journal of Logistics Management, 3*(26), 642–656.

Chen, J., Sohal, A. S., & Prajogo, D. L. (2013). Supply chain operational risk mitigation: A collaborative approach. *International Journal of Production Research, 51*(7), 2186–2199.

Chopra, S., & Sodhi, M. S. (2004). Managing risk to avoid supply chain breakdown. *MIT Sloan Management Review, 46*(1), 53–61.

Chopra, S., & Sodhi, M. S. (2014). Reducing the risk of supply chain disruptions. *MIT Sloan Management Review, 55*(3), 73.

Christopher, M., & Holweg, M. (2011). Managing supply chains in the era of turbulence. *International Journal of Physical Distribution & Logistics Management, 41*(1), 63–82.

Christopher, M., & Peck, H. (2004). Building the resilient supply chain. *International Journal of Logistics Management, 15*(2), 1–13.

Christopher, M., & Towill, D. R. (2001). An integrated model for the design of agile supply chains. *International Journal of Physical Distribution and Logistics Management, 31*(4), 235–246.

Das, K. (2011). Integrating effective flexibility measures into a strategic supply chain. *European Journal of Operational Research, 211,* 170–183.

Das, K., & Lashkari, R. S. (2015). Risk readiness and resiliency planning for a supply chain. *International Journal of Production Research, 53*(22), 6752–6771.

Dominik, E., Matthias, G., Constantin, B., & Michael, L. (2015). The performance impact of supply chain agility and supply chain adaptability: The moderating effect of product complexity. *International Journal of Production Research, 53*(10), 2–44.

Faisal, M. N., Banwet, D. K., & Shankar, R. (2006). Mapping supply chains on risk and customer sensitivity dimensions. *Industrial Management and Data Systems, 106,* 878–895.

Fang, H., Li, C., & Xiao, R. (2012). Supply chain network design based on brand differentiation and resilient management. *Journal of Information & Computational Science, 9*(14), 3977–3986.

Ghadge, A., Dani, S., & Kalawsky, R. (2012). Supply chain risk management: Present and future scope. *International Journal of Logistics Management, 23*(3), 313–339.

Gligor, D. M., Esmark, C. L., & Holcomb, M. C. (2015). Performance outcomes of supply chain agility: When should you be agile? *Journal of Operations Management, 33*(34), 71–82.

Gold, S., Seuring, S., & Beske, P. (2010). The constructs of sustainable supply chain management: A content analysis based on published case studies. *Progress in Industrial Ecology: An International Journal, 7*(2), 114–137.

Gunasekaran, A., Patel, C., & Tirtiroglu, E. (2001). Performance measures and metrics in a supply chain environment. *International Journal of Operations and Production Management, 21*(1/2), 71–87.

Hendricks, K., & Singhal, V. (2005). An empirical analysis of the effect of supply chain disruptions on long-run stock price performance and equity risk of the firm. *Production and Operations Management, 14*(1), 25–53.

Hendricks, K. B., & Singhal, V. R. (2003). The effect of supply chain glitches on shareholder wealth. *Journal of Operations Management, 21,* 501–522.

Ho, W., Zheng, T., Yildiz, H., & Ta, S. (2015). Supply chain risk management: A literature review. *International Journal of Production Research, 53*(16), 5031–5069.

Ismail, H. S., & Sharifi, H. (2006). A balanced approach to building agile supply chains. *International Journal of Physical Distribution & Logistics Management, 36*(6), 431–444.

Jain, V., Kumar, S., Soni, U., & Chandra, C. (2017). Supply chain resilience: Model development and empirical analysis. *International Journal of Production Research*, 1–22.

Johnson, M., & Templar, S. (2011). The relationships between supply chain and firm performance: The development and testing of a unified proxy. *International Journal of Physical Distribution & Logistics Management, 41*(2), 88–103.

Jüttner, U., & Maklan, S. (2011). Supply chain resilience in the global financial crisis: An empirical study. *Supply Chain Management: An International Journal, 16*(4), 246–259.

Jüttner, U., Peck, H., & Christopher, M. (2003). Supply chain risk management: Outlining an agenda for future research. *International Journal of Logistics, 6*(4), 197–210.

Kamalahmadi, M., & Parast, M. (2015). Developing a resilient supply chain through supplier flexibility and reliability assessment. *Intronational Journal of Production Research, 54,* 302–321.

Kamalahmadi, M., & Parast, M. (2016). A review of the literature on the principles of enterprise and supply chain resilience: Major findings and directions for future research. *International Journal of Production Economics, 171,* 116–133.

Kamalahmadi, M., & Parast, M. M. (2017). An assessment of supply chain disruption mitigation strategies. *International Journal of Production Economics, 184*(2017), 210–230.

Kilubi, I. (2016). The strategies of supply chain risk management—A synthesis and classification. *International Journal of Logistics Research and Applications, 19*(6), 604–629.

Kleindorfer, P. R., & Saad, G. H. (2005). Managing disruption risks in supply chains. *Production and Operation Management, 14*(1), 53–68.

Li, G., Fan, H., Lee, P. K., & Cheng, T. C. (2015). Joint supply chain risk management: An agency and collaboration perspective. *International Journal of Production Economics, 164,* 83–94.

Li, J., & Chan, F. T. (2012). The impact of collaborative transportation management on demand disruption of manufacturing supply chains. *International Journal of Production Research, 50*(19), 5635–5650.

Li, X., Goldsby, T. J., & Holsapple, C. W. (2009). Supply chain agility: Scale development. *International Journal of Logistics Management, 20*(3), 408–424.

Lim, M. K., Mak, H. Y., & Shen, Z. J. (2017). Agility and proximity considerations in supply chain design. *Management Science, 63*(4), 1026–1041.

Mandal, S. (2014). Supply chain resilience: A state-of-the-art review and research directions. *International Journal of Disaster Resilience in the Built Environment, 5*(4), 427–453.

Merschmann, U., & Thonemann, U. W. (2011). Supply chain flexibility, uncertainty and firm performance: An empirical analysis of German manufacturing firms. *International Journal of Production Economics, 130,* 43–53.

Narasimhan, R., Swink, M., & Kim, S. W. (2006). Disentangling leanness and agility: An empirical investigation. *Journal of Operations Management, 24,* 440–447.

Nooraie, S. V., & Parast, M. M. (2015). A multi-objective approach to supply chain risk management: Integrating visibility with supply and demand risk. *International Journal of Production Economics, 161,* 192–200.

Nooraie, S. V., & Parast, M. M. (2016). Mitigating supply chain disruptions through the assessment of trade-offs among risks, costs and investments in capabilities. *International Journal of Production Economics, 171*(1), 8–21.

Nyamah, E. Y., Jiang, Y., Feng, Y., & Enchill, E. (2017). Agri-food supply chain performance: An empirical impact of risk. *Management Decision, 55*(5), 872–891.

Overby, E., Bharadwaj, A., & Sambamurthy, V. (2006). Enterprise agility and the enabling role of information technology. *European Journal of Information Systems, 15*(2), 120–131.

Patel, P. C., Terjesen, S., & Li, D. (2012). Enhancing effects of manufacturing flexibility through operational absorptive capacity and operational ambidexterity. *Journal of Operations Management, 30,* 201–220.

Paulraj, A., & Chen, I. J. (2007). Environmental uncertainty and strategic supply management: A resource dependence perspective and performance implications. *The Journal of Supply Chain Management, 43*(3), 29–42.

Peck, H. (2004). Understanding the sources and drivers of supply chain risk. In S. Crainer (Ed.), *The financial times handbook of management* (3rd ed.). London: Pearson Publishing.

Pettit, T. J., Croxton, K., & Fiksel, J. (2013). Ensuring supply chain resilience: Development and implementation of an assessment tool. *Journal of Business Logistics*, *34*(1), 46–76.

Purvis, L., Gosling, J., & Naim, M. M. (2014). The development of a lean, agile and le-agile supply network taxonomy based on differing types of flexibility. *International Journal of Production Economics, 151*(1), 100–111.

Quang, H. T., & Hara, Y. (2017). Risks and performance in supply chain: The push effect. *International Journal of Production Research, 56*(4), 1369–1388.

Quang, H. T., Sampaio, P., Carvalho, M. S., Fernandes, A. C., An, D. T., & Vilhenac, E. (2016). An extensive structural model of supply chain quality management and firm performance. *International Journal of Quality & Reliability Management, 33*(4), 444–464.

Revilla, E., & Saenz, M. J. (2017). The impact of risk management on the frequency of supply chain disruptions: A configurational approach. *International Journal of Operations & Production Management, 37*(5), 557–576.

Ritchie, B., & Brindley, C. (2007). Supply chain risk management and performance: A guiding framework for future development. *International Journal of Operations & Production Management, 27*(3), 303–322.

Sanchez, A. M., & Perez, M. (2005). Supply chain flexibility and firm performance: A conceptual model and empirical study in the automotive industry. *International Journal of Operations & Production Management, 25*(7), 681–700.

Schoenherr, T. (2010). Outsourcing decisions in global supply chains: An exploratory multi-country survey. *International Journal of Production Research, 48*(2), 343–378.

SCRLC. (2011). *Supply chain risk management: A compilation of best practices.*

Sheffi, J. (2005). Building a resilient supply chain. *Harvard Business Review, 1*(8), 1–4.

Sheffi, Y., & Rice, J. B. (2005). A supply chain view of the resilient enterprise. *MIT Sloan Management Review, 47*(1), 41–48.

Shekarian, M., & Parast, M. (2018). The effect of supply chain disruption risks on organizational performance: A literature review. *North Carolina A&T State University, Greensboro, NC* (Working paper).

Simatupang, T. M., & Sridharan, R. (2005). The collaboration index: A measure for supply chain collaboration. *International Journal of Physical Distribution & Logistics Management, 35*(1), 44–62.

Sodhi, M. S., Son, B. G., & Tang, C. S. (2012). Researchers' perspectives on supply chain risk management. *Production and Operations Management, 21*(1), 1–13.

Stevens, G. (1989). Integrating the supply chain. *International Journal of Physical Distribution and Materials Management, 19*(1), 3–8.

Stevenson, M., & Spring, M. (2007). Flexibility from a supply chain perspective: Definition and review. *International Journal of Operations & Production Management, 27*(7), 685–713.
Sundram, V. P., Chandran, V. G., & Bhatti, M. A. (2016). Supply chain practices and performance: The indirect effects of supply chain integration. *Benchmarking: An International Journal*, *23*(6), 1445–1471.
Swafford, P. M., Ghosh, S., & Murthy, N. (2008). Achieving supply chain agility through IT integration and flexibility. *International Journal of Production Economics, 116*(2), 288–297.
Tang, C. S. (2006). Perspectives in supply chain risk management. *International Journal of Production Economics, 103*(2), 451–488.
Tang, C., & Tomlin, B. (2008). The power of flexibility for mitigating supply chain risks. *International Journal of Production Economics, 116*(1), 12–27.
Tang, O., & Musa, S. (2010). Identifying risk issues and research advancements in supply chain risk management. *International Journal of Production Econnomics, 133*(1), 25–34.
Thun, J. T., & Hoenig, D. (2011). An empirical analysis of supply chain risk management in the German automotive industry. *International Journal of Production Economics, 131,* 242–249.
Tomlin, B. (2006). On the value of mitigation and contingency strategies for managing supply chain disruption risks. *Management Science, 52*(5), 639–657.
Tukamuhabwa, B. R., Stevenson, M., Busby, J., & Zorzini, M. (2015). Supply chain resilience: Definition, review and theoretical foundations for further study. *International Journal of Production Research, 53*(18), 5592–5623.
Viswanadham, N. (2018). Performance analysis and design of competitive business models. *International Journal of Production Research, 56*(1–2), 983–999.
Viswanadham, N., & Samvedi, A. (2013). Supplier selection based on supply chain ecosystem, performance and risk criteria. *International Journal of Production Research, 51*(21), 6484–6498.
Wagner, S. M., & Bode, C. (2008). An empirical examination of supply chain performance along several dimensions of risk. *Journal of Business Logistics, 29*(1), 307–325.
Yang, Y., Pan, S., & Ballot, E. (2017). Mitigating supply chain disruptions through interconnected logistics services in the physical internet. *International Journal of Production Research, 55*(14), 3970–3983.
Zhu, Q., Krikke, H., & Caniels, M. C. (2017). Integrated supply chain risk management: A systematic review. *The International Journal of Logistics Management, 28*(4), 1123–1141.
Zsidisin, G. (2003). Managerial perceptions of supply risk. *Journal of Supply Chain Management, 39*(1), 14–26.
Zsidisin, G. A., & Ellram, L. M. (2003). An agency theory investigation of supply risk management. *Journal of Supply Chain Management, 39*(2), 15–27.
Zsidisin, G. A., Ellram, L. M., Carter, J. R., & Cavinato, J. L. (2004). An analysis of supply risk assessment techniques. *International Journal of Physical Distribution & Logistics Management, 34*(5), 397–413.
Zsidisin, G. A., Petkova, B. N., & Dam, L. (2016). Examining the influence of supply chain glitches on shareholder wealth: Does the reason matter? *International Journal of Production Research*, *54*(1), 69–82.
Zsidisin, G., Ragatz, G., & Melnyk, S. (2005). The dark side of supply chain management. *Supply Chain Management Review, 9*(2), 46–52.
Zsidisin, G. A., & Wagner, S. M. (2010). Do perceptions become reality? The moderating role of supply chain resiliency on disruption occurrence. *Journal of Business Logistics, 31*(2), 1–20.

Part VI
Grounding Our Understanding of Supply Chain Risk: Cases and Observations

Chapter 22
The Management of Disruption Supply Risks at Vestas Wind Systems

Chris Ellegaard and Anne Høj Schibsbye

1 Introduction

Vestas is the largest specialized wind turbine producer in the world. In a global industry characterized by continuous pressure to reduce costs of energy, project production and deliveries, advanced integrated wind turbine designs, long lead times, and delivery penalties from final customers, as well as complex logistics flows, supply risk management has become one of the most critical strategic tasks for Vestas. In this chapter, we zoom in on one critical supply risk category: supply disruptions. The literature has reported extensively on supply disruptions, but so far mostly in a generic manner, frequently proposing the same standard strategies for disruption risk regardless of the type of disruption. Only relatively few studies have started to open the black box of supply disruption risk (e.g., Chopra and Sodhi 2014; Ellis et al. 2011; Kleindorfer and Saad 2005). We extend on these studies by demonstrating how Vestas faces a wide variety of different supply disruptions, caused by sets of risk drivers that vary between the different supply categories. Through an analysis of three key supplies at Vestas: gearboxes, towers, and electronics, we show how these differences make Vestas managers choose very different mitigation strategies to successfully manage the various disruption risks. Based on the findings, we propose a simple supply disruption management framework, which can be used to identify the

Additional valuable insights for the chapter were provided by the following Vestas employees: supply risk management specialist Lukasz Kubiszewski-Jakubiak, category director towers Per Vanghøj Andersen, and category director gearboxes Jeppe Søndergaard.

C. Ellegaard (✉)
Aarhus University, Aarhus, Denmark
e-mail: chrel@mgmt.au.dk

A. H. Schibsbye
Electrical, Global Procurement, Vestas Wind Systems A/S, Aarhus, Denmark
e-mail: annho@vestas.com

G. A. Zsidisin and M. Henke (eds.), *Revisiting Supply Chain Risk*, Springer Series in Supply Chain Management 7, https://doi.org/10.1007/978-3-030-03813-7_22

drivers of disruption events and match them with the appropriate sets of disruption management strategies. As noted by Ritchie and Brindley (2007), supply chains are in many ways unique, and therefore, unique strategies are required to manage them.

2 Vestas and the Wind Turbine Industry

Wind turbines are huge, complex structures, consisting of blades, nacelle (housing), tower, and a foundation. The blades are installed on a shaft, which is located in the nacelle high above the ground, on top of the tower. The wind rotates the shaft with the blades, which drive a generator that produces green energy. Wind turbines may be installed at sea or on land, often in remote, but windy areas. Producers typically deliver entire wind turbine parks on a project basis, based on orders won through large-scale energy tenders. Servicing of the parks may be included in the sales. With more than 87 GWs out of the industry's 487 GWs of installed turbines globally, Vestas is a key player in the industry. Following some financial difficulties starting more than a decade back, Vestas turned around and has been growing since 2012, with 2017 reaching a record 10.5 GWs of orders (installed wind turbine capacity). Vestas employs more than 21,000 people, and revenues are expected to be around EUR 10bn for 2017, with an EBIT of approximately 12%. Vestas spend with external suppliers amounted to more than EUR 7bn in 2017, which emphasizes the importance of effective purchasing and supply chain management, including supply risk management.

Wind turbine production is highly specialized for a large part, and suppliers, producers, and customers can be found in any corner of the world. Besides Vestas, the industry is populated by several large players such as GE, Siemens Gamesa, and Goldwind, as well as many smaller companies. Vestas also competes for orders with companies in the broader green energy sector, comprising solar and hydropower solutions. In general, the industry faces a continuous hunt for reduced costs of energy in order to compete with not only traditional energy sources such as oil and gas, but also to remain the most cost-effective green energy provider. As a result, Vestas must continuously make their supply chain faster and more efficient and optimize processes and product designs, which increase the exposure to risks, including supply disruptions. Vestas has therefore made risk management a top strategic priority, and the company continues to improve risk management capabilities.

3 The Management of Disruption Supply Risk

Craighead et al. (2007, p. 132) define supply disruptions as "*unforeseen events that interfere with the normal flow of materials and/or goods within the supply chain*." As one of the major types of supply risk, disruptions result in losses for the focal company by fully or partly interrupting incoming supplies, hindering internal production, and possibly causing delays in delivering to customer markets. Disruptions may be caused by a wide variety of core causes including bankruptcy, terrorism, natural disasters, labor disputes, machine breakdowns, failing supplier capabilities, or deliberate supplier acts (Chopra and Sodhi 2004; Manuj and Mentzer 2008).

3.1 Disruption Risk Management Strategies

The most prevalent strategies to mitigate disruption risk are inventories and dual sourcing or redundant suppliers (Chopra and Sodhi 2004). These strategies are reactive, allowing the company to rely either on alternative suppliers or a component buffer in case a source fails. Companies may also operate a high level of flexibility or responsiveness in various parts of its supply chain operations, for instance keeping its own flexible production capacity or relying on possibly faster alternative transportation modes, such as air freight in case the supply chain is interrupted (Chopra and Sodhi 2004; Tang 2006). In- and outsourcing may be a more lasting solution to disruption risk. Vulnerable processes subject to capacity shortages may be insourced, for example (Manuj and Mentzer 2008). Reversely, outsourcing may have the same effect, transferring the risk of disruption to suppliers with a particularly robust supply chain setup. Hedging is another frequent disruption management strategy, which involves scattering the sources of supply, either suppliers or their individual facilities, across global geographical locations, avoiding the vulnerability of centralized production nodes (Manuj and Mentzer 2008). Chopra and Sodhi (2014) recently argued for another supply chain design strategy, namely regionalizing supply chains. By setting up several regional supply chains with sources closer to customers for each region, companies hedge supplies, while shortening the supply chain, leading to a lower response time in case of disruptions and at lower logistics costs. The more regional or local the source, the faster the reaction time in case of disruptions (Ellegaard 2008).

Disruptions may also be mitigated through postponement strategies, producing a generic product based on overall demand and then postponing the customization, which enables a faster disruption recovery (Tang 2006). Standardization of components also allows a broader supply base and more options for relying on alternatives in case of disruption. The final category of supply disruption management strategies can be grouped under the heading behavior-based strategies (Zsidisin and Ellram 2003). Behavior-based strategies such as supplier development alter suppliers' capabilities, causing improved delivery performance, while strengthening the relationship to the supplier (Zsidisin and Ellram 2003). As such, they also improve the buying company's influence over key supplier decisions and access to risk information (Bode et al. 2011). Such influence is critical in disruptions where a key supplier's prioritization among customers in their portfolio is required, for example, when facilities or machinery is damaged due to natural disasters. Working to increase attractiveness and achieve preferred customer status with key suppliers also has disruption reducing effects (Reichenbachs et al. 2017).

3.2 *The Variety of Disruption Risks and the Strategies for Managing Them*

Extant research on supply disruption management has produced valuable insights but has not yet dealt much with the many considerable differences between different types of disruptions. For instance, a disruption caused by a fire in the supplier's factory, due to a port strike or due to a supplier's bankruptcy, is a markedly a different event and may require different risk management strategies. Chopra and Sodhi (2014) recently argued that segmentation of supplies in terms of, e.g., volumes, product variety, and demand uncertainty is required because variety of these dimensions point to different optimum risk management strategies. Both Craighead et al. (2007) and Kleindorfer and Saad (2005) went one step further and investigated the nature of different disruption hazards and connected these to particular mitigation strategies. In this chapter, we wish to extend further on these works by uncovering a wider range of disruption characteristics and connect them to particular viable strategies. Similar to Blackhurst et al. (2005), we wish to dive below the "big picture" and get into the specificities of disruptions. In order to gauge the characteristics of different types of disruptions, forming the basis for selecting the most viable risk management strategy, we adopt the following simple model (see Fig. 1).

The model, which is used for our subsequent discussion of different Vestas disruption strategies, is adapted from Ritchie and Brindley (2007), Ellis et al. (2011),

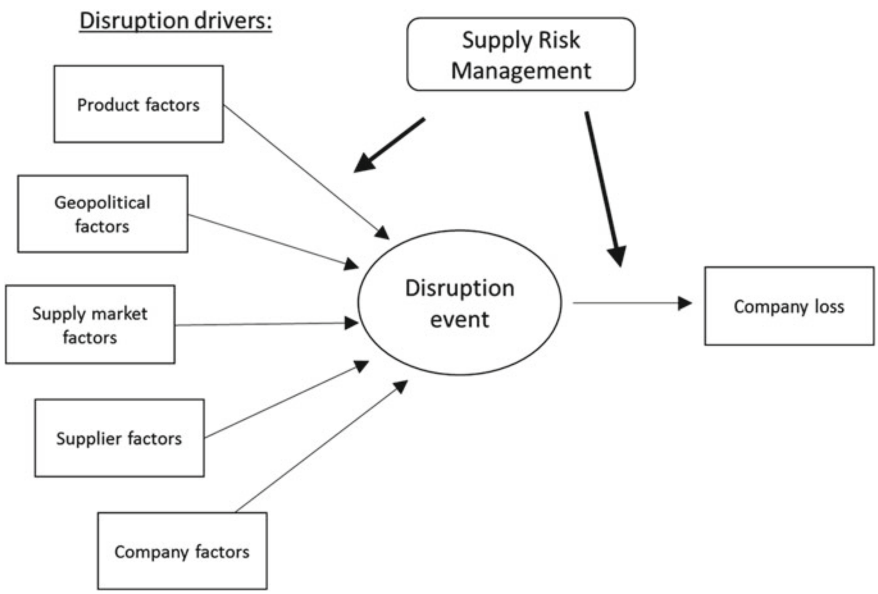


Fig. 1 Drivers of supply disruption risk based on Ritchie and Brindley (2007), Ellis et al. (2011), and Zsidisin and Wagner (2010)

and Zsidisin and Wagner (2010). Ritchie and Brindley (2007) point out that the uniqueness of each supply chain in terms of the drivers points to equally unique management strategies. We extend on the frameworks by opening up one type of risk and demonstrate the need for differentiated management strategies within this risk type.

4 Disruption Risk Management at Vestas

The Vestas supply risk management process, including supply disruption management, has two elements: (1) an overall risk intelligence and reporting system, which is developed and coordinated by supply risk specialists at the corporate level, and (2) specific risk management strategies and actions, which are managed at the category manager level and team level. The intelligence and reporting system is a highly formalized set of IT-based procedures that enable Vestas to identify key strategic risks, many of them originating in the upstream supply chain. Managers in different functions across Vestas, including procurement, are responsible for continuously identifying and reporting on observed risks through this system. Risks are analyzed on the likelihood and impact on finances and customers and are assigned a red, yellow, or green color code signaling their criticality. Red risks are escalated to a risk committee consisting of top executives, who evaluate and make decisions regarding mitigation. In addition, relevant supply chain VPs and the CPO can observe the critical risks. 50–100 risks may be in report at any given point in time, but only the most critical ones are escalated. Otherwise, the supply-related risks are mitigated by the procurement responsible (mostly category managers) assisted by their category teams. Making supply risk management part of the category team tasks ensures a coordinated effort that takes product development, production, as well as procurement, into account. There is also a tool and a template for initiating the mitigation of individually identified supply risks. The drivers and circumstances surrounding a given disruption risk vary from supply type to supply type, and the chosen mitigation strategies are therefore employed by the responsible category managers in combination with the category team, containing members from different Vestas functions, such as quality and product development. Table 1 shows the differences in driver profiles between three key supplies at Vestas indicating the level of criticality (drivers in left column refer to Fig. 1).

Below, we describe the disruption drivers for each of the three supplies and provide an overview of the applied disruption management strategies. For the electronics category, we have added a brief disruption case and describe how Vestas used the learnings from this case to alter their disruption management approach.

Table 1 Different disruption driver profiles of key Vestas supplies

	Gearboxes	Towers	Electronics
Product	High	High	Low
Geopolitical	Low	Medium	Medium
Supply market	High	Low	High
Supplier	Low	High	Low
Vestas	Medium	High	Low

4.1 Gearboxes

The gearbox, which is located in the nacelle on top of the tower, is one of the largest components in the wind turbine and has a long product development and qualification time. The gearbox is also a production bottleneck with very long lead times. Any disruption of this complex supplied system can therefore have heavy consequences, so a foolproof design process and a well-functioning quality management system are therefore required. Vestas' narrow nacelle design places strict demands on suppliers' technological capabilities, and only a limited number of suppliers globally are regarded capable of supplying this key product. It is a hi-tech product, with a huge effect on the wind turbine's ability to compete in a market becoming more and more focused on the costs of energy. To deliver more energy cheaper, wind turbines are growing in size, which requires increasingly larger blades and more effective gearboxes. First-tier suppliers are quite stable *geopolitically*. Some second-tier suppliers may be exposed, although not critically. For example, large-scale steel production tends to pollute, which at present has caused the Chinese government to close down steel producing factories, and this has affected second-tier Vestas suppliers. Historically, suppliers have also occasionally been faced with new import taxes. However, overall this risk driver category has a relatively low criticality for gearboxes. The *supply market* was earlier populated by a broader range of gearbox suppliers, but several acquisitions have reduced the number of companies on the market. Mergers, acquisitions, and alliances have been frequent in this part of the industry, increasing the vulnerability of wind turbine producers. Today the majority of wind turbine producers use the same limited number of suppliers, and there are often no real alternatives. Vestas presently uses only a few large gearbox suppliers in a setup with high mutual interdependence. Given the high level of specialization, the risk of major customers from other industries stealing the suppliers' attention is quite small. However, Vestas shares these suppliers with other wind turbine producers, who also have very close connections to them.

The present *suppliers* are large well-run companies with considerable operational and technical capabilities. The most prominent threat in this driver category is a potential takeover of a key gearbox supplier by a wind turbine competitor, and such industry moves have been relatively frequent in the industry historically. Such a change could threaten Vestas' ability to deliver in situations of capacity constraints, or

Vestas could be forced to look for other supplier solutions to protect their intellectual property. Given the customized designs and lengthy design processes, the switching time and costs would be high. Finally, *Vestas* has historically made a few risk-enhancing gearbox decisions, such as estimating supply market capacity inaccurately or linking too closely with an incapable single source. Their strategic choice of relying on suppliers for this key component rather than own production could also be perceived as such a driver. However, Vestas-caused disruption drivers are generally perceived as quite low.

Supply Risk Management of Gearboxes
When looking at categories characterized by a relatively narrow supply base with only a few suppliers, Vestas is always evaluating the supply market. Knowledge about new potential suppliers must be obtained in case it becomes relevant to introduce a new alternative supplier, as development and qualification time is very long. In addition, developing a new supplier requires a considerable amount of invested resources, but high supply risk management benefits can be expected, including the full attention from new suppliers. In addition, Vestas is heavily focused on monitoring the supply market for acquisition activity. They are motivating employees to pick up signals from the market and their network, and they monitor financial market movements. Acquisition risk is assigned a red lamp in the Vestas supply risk management warning system and is watched continuously. Vestas' top management also builds close relations and has frequent talks with their suppliers' top management regarding the future market movements, among other things. Vestas also has contracts covering critical areas such as IPR, capacity and delivery commitments, inventory regulation, and forecast management.

4.2 Towers

The wind turbine nacelle with the rotating blades is positioned on top of the tower, which is manufactured in modules and then assembled on the final wind turbine site. The tower is a *product* design with many parts, the most important being milled steel plates (comprising the tube shell), as well as various internal components such as platforms, flanges, stairwells, doors, service lifts, and cables. It is not a complicated or highly technological product, but with the massive size and weight of both the final tower (sometimes higher than 150 m) and the modules, transport is a critical supply risk management factor. Sea or railway transport is the standard, truck is possible but problematic, and air transport is not feasible. Unlike most competitors, Vestas customizes its tower design to specific customer orders (parks with a high number of turbines). This customization creates options for optimizing performance and taking out material costs, but it also affects disruption risk management options. *Geopolitically*, towers have a relatively low level of exposure to supply risk. Unlike gearboxes and electronics, towers are frequently subject to national law demands for local content, which requires the use of suppliers originating in the same country as the customer (approximately half of the customer locations are subject to this demand at present). Vestas therefore operates a broad range of suppliers from different parts of the world, which makes their exposure to natural or political disruption events at one particular location low. However, sometimes the steel prices, currencies, and labor costs, etc., in one supplier location may be so beneficial that Vestas wants to rely more on these local suppliers for a larger part of their business, despite longer transport. In a few instances, such locations have been threatened geopolitically, and Vestas must then carefully evaluate and balance geopolitical risks with the rewards from ramping up with specific suppliers. The global towers *supply market* is even more expanded than the electronics supply market. The world market is populated by a host of companies that can manufacture the towers, and global capacity is rarely a problem. Vestas has its own huge production facility in Colorado, USA, but this is mainly to cover the regional market. Mainly because of the local content demand, they source from 52 different suppliers that cover all global locations, including some that are not in use but are approved to do the job. The drivers connected to the specific *suppliers* are more critical for Vestas. With a large range of different suppliers, Vestas is highly exposed to risk originating within each of these suppliers. Hence, disruptions caused by quality or financial issues are more likely. A specific supplier may fail to maintain its quality management, or it may come to lack finances to invest in machinery to cater for increasing size demands facing the wind turbine industry. Bankruptcy may even be a threat to some suppliers, and due to the high number of suppliers, it is difficult for Vestas to be informed about the state of each individual supplier. Finally, *Vestas*' own deliberate strategies, although highly beneficial from a broader business perspective, are actually critical supply risk drivers. The strategy of customizing the towers for each individual order means that reserves such as inventories (and to some extent reserve suppliers) are largely excluded as risk management options. In fact, past financial difficulties, partly caused by excessive inventories, made Vestas' top management decide that inventories are generally unwanted. Exposure to disruption risk is therefore magnified for towers.

Supply Risk Management of Towers

Given the high exposure of Vestas, monitoring has become an integrated part of their supply risk management effort. Vestas audits each tower supplier annually on quality and twice annually on finances. Since this is a resource demanding task, they are presently working on establishing partnerships with 4–6 key suppliers. These suppliers are strong players in the industry and capable of following Vestas into new markets, where they can either establish their own facilities or establish joint ventures with local suppliers. This way, Vestas can maintain global coverage with multiple sources, but with less exposure to individual supplier risk. They are simultaneously strengthening relationships with these suppliers, on the one hand, to motivate the flexibility of these suppliers and on the other hand, having a positive effect on all aspects of disruption risk. Vestas is also using contracting to mitigate tower disruption risk because demand on new wind energy customer markets may sometimes take off quite fast, with competitors seeking capacity from the same suppliers. Furthermore, Vestas discusses business development with tower suppliers and subsequently asks them to commit contractually, for example, on investment requirements and market coverage. Finally, Vestas is discussing various types of postponement strategies with key suppliers, allowing faster reaction in case of disruptions.

5 Electronics

Vestas uses electronics for various types of controls, ranging from the central nacelle-placed control of the rotating blades to decentral controls, such as deicing controls placed within the blades. When it comes to electronics, understood here as components to be mounted on printed circuit boards, Vestas' supply risk management task has some similarities with that of the many other companies, across various industries, that incorporate electronics as key components in their product. Starting with the *product* itself, these are mostly relatively low cost, standard components with low complexity, and their small size makes many aspects of transportation easy. One influential product factor is the high pace of technological development, which has an effect on the viability of some types of disruption management strategies. *Geopolitical* factors are of medium criticality. Electronics are produced in a worldwide supply market, which is not plagued by political factors overall, but a significant part of the production capacity is placed in regions vulnerable to natural disasters, for example, various Asian locations. Although the *supply market* is massive with considerable capacity dispersed between a large range of producers and distributors, it is also characterized by a recurrent periodical mismatch between supply and demand, known as "allocation." During allocation, global demand exceeds supply, and the likelihood of disruption increases manifold. Essentially, Vestas regularly finds themselves in competition with other electronics buyers across industries to secure supplies of these vital components. For example, sometimes suppliers are suddenly not able to deliver the promised volumes because demand from other customers and industries increases to such an extent that it drives the supply market into a situation of shortage. This results in serious competition for supplies, where volumes are one of the most significant parameters. With the relative low volumes of Vestas, relative to automotive OEMs, for example, it leaves the company in a critical situation. In addition, the delivery time of many electronic components is often extremely long, approaching one year for particular types. Moreover, supply and demand are exceedingly difficult to monitor and assess, especially further upstream, because it relies on a broad range of complicated macro-factors, and the vast number of companies in this industry are tied together in a complex net of agreements and commitments with very limited transparency. Concerning the fourth group of drivers, *supplier* characteristics, Vestas buys from a mixture of generally competent electronics producers and distributors, and disruptions originating within the suppliers' organizations are therefore rare. Finally, *Vestas'* own internal capabilities may affect possible supply disruptions on electronic components, although to a limited extent. The ability to forecast, perform production planning, and be in control of stock levels are critical drivers of electronics disruptions.

5.1 *Electronics Case—Earthquake Damages to a Key Supplier's Production Facility*

Vestas has faced a range of different disruption risks during the past years. One particularly challenging disruption occurred, when an earthquake damaged a production facility of a key electronics supplier. Vestas' corporate risk intelligence and reporting system picked up notices from the media within a day of the earthquake, leading to the quick initiation of an assessment procedure among members of the purchasing organization. The assessment identified five suppliers in the area, out of which four could not have been impacted by the earthquake. Unfortunately, the final supplier in the area was struck by the earthquake. Moreover, this supplier delivered an older generation of key components to Vestas, maintained through multiple lines of wind turbine designs due to its solid performance. Most competing wind turbine producers had substituted this component in their new designs, leaving Vestas as one of the only customers in the industry for this particular component.

Picking up the bad news, purchasing managers attempted to contact their counterparts in the supplier organization to get further information for a more accurate assessment. These efforts were only somewhat successful, with supplier employees confirming that production lines were only partly damaged with considerable capacity still up and running, but otherwise claiming that they had not yet formed an overview of the damages, and asking for no further visits and wanting to keep communication limited. Vestas quickly realized that alternative capacity was difficult to find due to the outdated design and upon asking the supplier to free capacity on one of its other global facilities they learned that this specialized component was not produced elsewhere—essentially only at the damaged facility.

In this early stage, speed was vital, and Vestas immediately started to redesign the component out of the relevant wind turbine models. They also knew from experience that other buyers would act in similar ways and figure out new design solutions, which would move allocation pressure onto these other components, making it a race to come up fast with viable redesigns. However, the redesign also took time and would therefore only solve needs from a given future start date. In the meantime, Vestas had started applying serious pressure on the supplier, sending employees to the production site and forcing the supplier to hold daily meetings with updates. On the one hand, they wanted to respect the supplier's request for time to solve the issue, but on the other hand, they wanted to be first in the queue for capacity. Vestas was not a key customer with this supplier, but they managed to get attention by cultivating the links of a close alliance partner into the supplier organization. They also attempted to use other suppliers to gain access to the supplier. Although small improvements were achieved on a daily basis with the supplier, the comparison of Vestas needs with conservative supplier estimates of supplier capacity still revealed large gaps in the upcoming period, starting when the supply pipeline would be emptied. Before redesigns were ready to be implemented, other tactics had to be attempted to avoid production stop and eventually failed deliveries, which would have critical financial consequences.

Addressing this issue, Vestas employed various strategies. First, they encouraged the supplier to come up with alternative production and logistics solutions, basically to get as many components through the supply chain as fast as possible. These joint solutions also solved a minor part of the problem. Eventually, Vestas had to go out on what is known as the "gray market" in electronics. This market is populated by companies that have earlier bought up specialized and/or obsolete components and placed them in inventory, in order to profit from it in these exact disruption situations. Some of these companies even contacted Vestas right after the disruption to offer the components. Others were located through Vestas key employees, with past careers in such companies. By gathering intelligence, Vestas also started to know other key customers for these specialized components from other industries. Despite large efforts, it became apparent that much of the lacking demand had to be covered through several of these "gray suppliers," at a high additional product price. Interestingly, quality, which is frequently an Achilles heel of electronics, also became an issue. Vestas feared that some of the gray market components would not be genuine or of suboptimal quality and therefore had to spend many additional resources for testing and quality checks. Finally, in order to avoid production stop, Vestas employed an assembly postponement tactic, whereby the production setup was changed to optimize the output, given the reduced inflow of components. All in all, a bothersome and costly process. However, through close supplier collaboration and considerable efforts across the supply chain, Vestas managed to avoid delivery failures for their customers and without needing to implement the new redesigns.

5.2 How These Experiences Led to Changes in Electronics Disruption Management

The above case is successful in terms of dealing with a very difficult disruption and actually avoiding failed deliveries to customers. However, Vestas' efforts were quite resource consuming, and purchasing executives and managers therefore subsequently started applying the learning from this and other disruption situations to improve future supply risk management procedures for electronics. Generally, catastrophe disruptions should not be managed 100% proactively because the costs of doing so are too high. However, Vestas wanted at least to make the process *more* proactive in terms of preparing even better for future similar disruptions. The first initiative was to make monitoring of critical components each category managers' task rather than relying merely on the general warning system combined with mostly reactive measures. This involved the assessment of each component in a category at regular intervals on a scale of low, medium, or high criticality and then making a risk management plan and strategy for each highly critical component.

Something that Vestas had already started changing well before this disruption was systems redesign to increase the level of standardization. Increased standardization would open up the range of possible sources, and it would increase the number of global production sites, both within and across individual suppliers, increasing the responsiveness of the supply base in case of disruptions. Vestas' new line of wind turbines held fewer and more standardized electronic components, and the aim was to incorporate these into the older lines also. This was a big ongoing effort, but through discussions between purchasing, R&D, and operations, they were making steady progress. Basically, "Vestas-specific" components were to be avoided if possible. However, for some key components, having a specific single source component can be a strategic choice and procurement would in such cases mitigate by applying logistics agreements with suppliers that guarantee supplies. Reducing the number of components and standardizing them also reduced obsolescence, a notorious electronics risk. For older specific electronic components and for components in already installed wind turbines with a service contract, Vestas ran an obsolescence team, who communicated closely with suppliers to know when components would go out of production and then prepared mitigation plans, for example, buying up components or discussing substitution possibilities with the supplier.

Other key focus areas for Vestas were improved customer attractiveness and relationship management. As a starting point, this would only be possible with a supply base consisting of a few key suppliers, rather than a large complex supply base, thereby enabling Vestas to increase their attractiveness with the remaining suppliers. For electronics, it had also become clear that they needed to increasingly cultivate solid supplier relationships with frequent visits and communication. Despite being a smaller player on the electronics market, compared to the major automotive and consumer electronics OEMs, Vestas believed that strengthened social relations would be vital for the future electronics supply disruption management. It would improve information exchange from specific suppliers in a global market, where supply and demand were very difficult to predict, increase the supplier's prioritization of Vestas, and ensure a smoother mitigation process in case of disruption events. Vestas also looked for other ways to increase attractiveness, for instance, bringing their insights from the green energy market, which was broadly considered a market with huge future potential for electronics producers, into play for key suppliers. However, Vestas had also realized that despite any efforts, they would, in all likelihood, continue to be down prioritized by some suppliers relative to larger customers from other markets. As a result, they considered outsourcing assemblies to specialized electronics assembly partners, who run this as their core business. As a more attractive account, Vestas could use the electronics market presence and expertise of the partner to absorb supply risks.

6 A Framework for Disruption Risk Management

Based on the analysis of the three different types of supplies, we suggest that companies adopt an analytical framework which recognizes the diversity within the disruption risk category. Different risk driver profiles cause different disruption events which require differentiated sets of mitigation strategies. Figure 2 shows the very

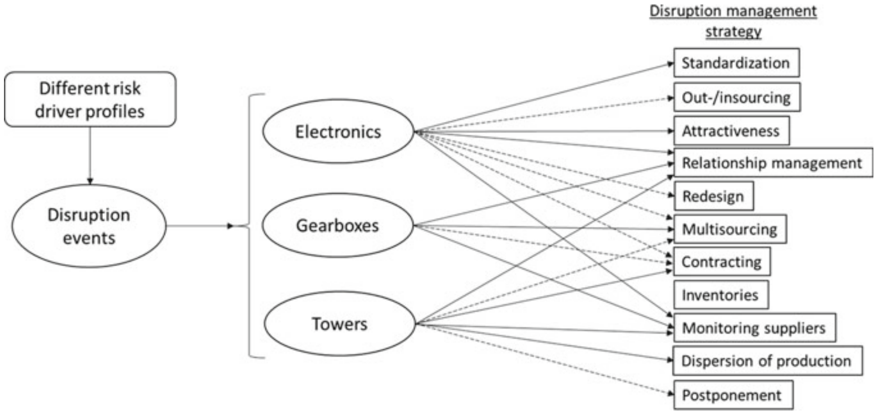


Fig. 2 A disruption management framework with examples from Vestas

different portfolios of disruption management strategies chosen for the three Vestas supplies. A solid line indicates a primary strategy, whereas a dotted line marks a secondary strategy.

We caution that other factors affect the optimum choice of disruption management strategies, including the costs of adopting the different strategies, interdependencies between strategies, and company-specific factors, such as corporate strategy and finances. However, given our focus on disruption drivers and management strategies, we have decided to leave these other factors out of the framework.

7 Conclusion

Most extant disruption management frameworks list generic mitigation strategies that seem to produce the same effect against any type of disruption. However, disruption events come in lots of different varieties, which have their roots in different sets of drivers. Not all disruption mitigation strategies are therefore equally effective, and companies must put together a portfolio of mitigation strategies that matches the exact form of disruption they are facing. In this chapter, we have laid out the different disruption management strategies of a MNC, which has adopted supply risk management as a core strategic priority. We have shown how Vestas successfully operates very different disruption mitigation strategies depending on the risk driver profile of a given supply, exemplified by the three key supplies gearboxes, towers, and electronics. These management efforts are supported by an advanced corporate risk intelligence and reporting system.

Despite the relatively high level of sophistication and a track record of successfully managing disruption supply risks, Vestas is working on raising the bar further. For example, they are implementing root cause analysis in the procurement organization, motivating employees to target the origins of disruptions. Further overall improvements in working relations with key suppliers are also on the agenda in order to improve upstream transparency and work with suppliers to mitigate risks. Vestas also wants to improve their supply risk management competencies for new product introductions. Assessment and management of possible supply risks should be incorporated already when new products are developed. Also, risk intelligence gathering and reporting should be better balanced with the actual mitigation. Vestas has succeeded in building a strong intelligence and reporting system, but the reporting should not take away resources from the actual mitigating actions. Finally, managers emphasize the need for an improved learning process that can systematically preserve knowledge of past supply risk management experiences and results, feeding into the continuous development of the supply risk management efforts at Vestas.

References

Blackhurst, J., Craighead, C. W., Elkins, D., & Handfield, R. B. (2005). An empirically derived agenda of critical research issues for managing supply chain disruptions. *International Journal of Production Research, 43*(19), 4067–4081.

Bode, C., Wagner, S. M., Petersen, K. J., & Ellram, L. M. (2011). Understanding responses to supply chain disruptions: Insights from information processing and resource dependence perspectives. *Academy of Management Journal, 54*(4), 833–856.

Chopra, S., & Sodhi, M. S. (2004). Managing risk to avoid supply-chain breakdown. *Sloan Management Review,* Fall, 53–61.

Chopra, S., & Sodhi, M. S. (2014). Reducing the risk of supply chain disruptions. *Sloan Management Review, 55*(3), 72–80.

Craighead, C., Blackhurst, J., Rungtusanatham, M., & Handfield, R. (2007). The severity of supply chain disruptions: Design characteristics and mitigation capabilities. *Decision Sciences, 38*(1), 131–156.

Ellegaard, C. (2008). Supply risk management in a small company perspective. *Supply Chain Management: An International Journal, 13*(6), 425–434.

Ellis, S. C., Shockley, J., & Henry, R. M. (2011). Making sense of supply disruption risk research: A conceptual framework grounded in enactment theory. *Journal of Supply Chain Management,* April, 65–96.

Kleindorfer, P. R., & Saad, G. H. (2005). Managing disruption risks in supply chains. *Production and Operations Management, 14*(1), 53–68.

Manuj, I., & Mentzer, J. T. (2008). Global supply chain risk management. *Journal of Business Logistics, 29*(1), 133–155.

Reichenbachs, M., Schiele, H., & Hoffman, P. (2017). Strategic supply risk: Exploring the risks deriving from a buying firm being of low importance for its suppliers. *International Journal of Risk Assessment and Management, 20*(4), 350–373.

Ritchie, B., & Brindley, C. (2007). An emergent framework for supply chain risk management and performance measurement. *Journal of the Operational Research Society, 58*(11), 1398–1411.

Tang, C. S. (2006). Robust strategies for mitigating supply chain disruptions. *International Journal of Logistics: Research and Applications, 9*(1), 33–45.

Zsidisin, G. A., & Ellram, L. A. (2003). An agency theory investigation of supply risk management. *Journal of Supply Chain Management,* Summer, 15–27.

Zsidisin, G. A., & Wagner, S. (2010). Do perceptions become reality? The moderating role of supply chain resiliency on disruption occurrence. *Journal of Business Logistics, 31*(2), 1–20.

Chapter 23
Foreign Exchange Risk Mitigation Strategies in Global Sourcing: The Case of Vortice SPA

Barbara Gaudenzi, Roberta Pellegrino, George A. Zsidisin and Claudio Bruggi

1 Introduction

Global supply chains are exposed to numerous risk sources stemming from their supply base, such as unexpected lead time variability, warehouse costs, capacity constraints, or fluctuations in purchase prices due to currency rate exchange volatility (Blackhurst et al. 2005; Yang and Yang 2010). Although research on global supply chain risk sources in the supply base has increased in recent years (Zsidisin and Wagner 2010; Jia and Zsidisin 2014), our understanding of currency rate exchange volatility, and the resulting foreign exchange (FX) risk firms are exposed to, is currently limited from a supply chain perspective. The purpose of this chapter is to present an illustrative case of how Vortice SpA, a medium-sized Italian producer of ventilation systems for residential and industrial applications, perceives and mitigates FX risk in their firm and extended supply chains.

B. Gaudenzi (✉)
Department of Business Administration, University of Verona, Verona, Italy
e-mail: barbara.gaudenzi@univr.it

R. Pellegrino
Department of Mechanical, Manangement and Mathematics, Polytechnic of Bari, Bari, Italy

G. A. Zsidisin
Department of Supply Chain Management and Analytics, Virginia Commonwealth University, Richmond, VA, USA

C. Bruggi
Vortice Elettrosociali SPA, Zoate, Milano, Italy

G. A. Zsidisin and M. Henke (eds.), *Revisiting Supply Chain Risk*, Springer Series in Supply Chain Management 7, https://doi.org/10.1007/978-3-030-03813-7_23

2 Foreign Exchange Risk Mitigation Strategies

Foreign exchange risk is defined as the risk of an investment's value fluctuation due to the changes in currency exchange rate, which can significantly affect profitability, organizational cash flow, and the ability to competitively price products (Burnside 2012). Numerous studies from the finance literature (Dufey and Srinivasulu 1983; Brown 2001; Chong et al. 2014) have provided insight into hedging strategies firms can adopt for mitigating the financial effects of currency rate volatility. However, there are few published research studies examining other approaches firms can consider in mitigating FX risk exposure in their supply chains (Bandaly et al. 2014; Caniato et al. 2016). An initial typology of FX risk mitigation strategies has been proposed by Zsidisin and Gaudenzi (2018), consisting of operating, financing, and contracting strategies.

Operating FX risk mitigation strategies are associated with investments in production and sourcing flexibility. Through production, flexibility organizations can switch production between plants with the scope to prevent or mitigate risks stemming from specific countries or production sites. Sourcing flexibility is related to the opportunity to have multiple sourcing in order to increase the reliability of the suppliers, including in response to changing currency valuations. *Financing FX risk mitigation strategies* are largely used in the forms of option contracts and forward contracts to reduce the negative impact of currency rate volatility on supply chain operations (Bandaly et al. 2014). As briefly discussed earlier, these have been more extensively studied within the finance literature. The third classification, *Contracting FX risk mitigation strategies,* considers approaches such as escalation/de-escalation clauses and payment terms in purchasing contracts to share the risk of currency rate volatility with suppliers.

An implied facet of these approaches is that they extend beyond the purview of one business function. The expertise from various business functions may be required in creating and pursuing operating, financing, and contracting FX risk management strategies. Finance is one function traditionally tasked to create financial hedging strategies (Brown 2001). However, marketing and purchasing serve as boundary spanning functions, respectively, for integrating with customers and suppliers, especially in developing and managing global supply chains. Due to their boundary spanning coordination with customers and suppliers from other countries, these business functions should serve a critical role in incorporating various risk elements in business transactions, including FX risk. In addition, legal serves a significant role in mitigating this form of risk, particularly regarding the laws and treaties within and among countries in conducting business transactions (Aggarwal and Goodell 2009).

3 Mitigating Foreign Exchange Risk at Vortice Elettrosociali SpA

The following case provides an example of strategies an Italian manufacturer considers in mitigating FX risk in its supply base. The case study consists of interviews conducted, in particular, with the Purchasing Director and the Vice CEO. The case starts with a background of Vortice and the ventilation industry. Global supply risk is then discussed, with a focus on the company's exposure to FX risk. Risk mitigation strategies utilized by Vortice are then presented with an example of how FX risk financially affects product cost structures.

3.1 Background

Vortice Elettrosociali SpA, a medium-sized Italian company, designs and produces ventilation systems for residential and industrial applications in global markets, with revenues of 60 million euro and 300 employees. Vortice purchases globally from more than 500 suppliers located in 30 countries including China, Turkey, South Korea, UK, and Far East regions. They have three production plants (two in Italy and one in China) and three commercial subsidiaries in France, UK, and Costa Rica.

Ventilation is a segment of the heating, ventilation, and air conditioning (HVAC) market, which is valued at about $95 billion USD. The primary drivers of the HVAC market include the number of new households, construction spending, and rapid urbanization in emerging economies. Opportunities in this industry include having great demand for energy-efficient systems, the increasing trend of smart homes, and implementing green technologies. The market is characterized by high volumes and average margins, with demand trends being influenced by weather conditions and seasonality. Key strategic challenges are therefore demand planning and cost analysis across the global supply chain.

Management at Vortice recognizes and systematically manages several supply risks, with the scope to protect the organization in terms of reliability in lead times, quality issues, quality of the supplied goods, and information sharing with suppliers. Two key tasks in Vortice's purchasing department are the management of *relationships with suppliers*, investing in information sharing and stable relationships, and careful *negotiation with suppliers* about service and cost issues.

3.2 FX Risk at Vortice

One risk that is considered increasingly relevant in global purchases is FX risk. Vortice purchases in US Dollars (USD) from several medium and large-sized suppliers, which operate in the ventilation and air conditioning supply chain as channel leaders,

Table 1 Interview highlights on FX risk in global purchasing

Theme	Highlights
FX risk in global purchasing	"FX risk is a "small piece" of the global purchasing strategy, but it is relevant in terms of costs and is difficult to manage"
Key issues related to FX risk	"Even though Vortice is a small company, we have a couple of issues related to FX risk: first, we buy some components or some products that we directly commercialized in USD and for which we don't have alternative manufacturers in EU. Second, our product is a seasonal product: if you have the product at the right time, we can sell it, otherwise you don't have demand… If Vortice misses the FX rate at a certain point of time (one month), we lose a big part of profitability even for the reason that of course if you buy and sell you don't have a lot of margin and the purchasing power with suppliers is generally low"
FX risk and total cost of products	"FX risk matters especially with low margin products, with very long lead time from order to final delivery, particularly when large investments in inventories are not possible" "Transfer price is a very big problem. First, we manage the sales using the price list that is stable for at least 6 months: if you make the wrong choice we need to redefine the proper transfer price. Second, the Tax Authority checks the profitability of your intragroup clients afterwards, if you set the price at the beginning of the year with a correct margin, but at the end of the year the margin collapses due to FX fluctuations, the Tax Authority does not care"

and also trade components and ventilation accessories from the UK in British Pounds (GBP). Most FX risk exposure exists with China in USD (about 4.5 million USD) and with the UK market in GBP (less than 1 million GBP per year).

FX risk is difficult to manage at Vortice for several reasons. First, Vortice mainly sells seasonal products that need to be available to meet customer demand. Second, the high level of customization of Vortice products creates extended sourcing lead times. The process starts with the purchase of the components/products in October/November, followed by their shipment in December/January and their receipt in February/March. The end product is then sold to electrical wholesalers that in turn serve installers which install the product at the final user's house. Finally, due to the high size and level of customization of its products, Vortice cannot manage seasonality effects through inventory management. The complexity of the production process increases Vortice's exposure to FX fluctuations. For this reason, managers are paying increasing attention to FX risk analysis and mitigation, as highlighted in the key themes summarized in Table 1.

3.3 FX Risk Exposure Analysis

FX risk exposure can significantly affect cost structures, which are measured by using simulations of the price and volume variance and their effects. During the budgeting process, the company fixes the Standard FX rate for the next year, and based on this, all other standard costs are estimated (labor and raw materials, excluding overhead). Then, Vortice periodically monitors all the cost components as well as volume and calculates the influence of each factor on the total variance of the margin compared to the budget. When the FX rate fluctuations penalize the business, either for Vortice or for suppliers, the prices are renegotiated, without a predefined fixed frequency. Using the breakdown cost approach, the reliability of these evaluations covers approximately 75–80% of the total spent in terms of value. More than 2500 items are investigated in terms of cost structure, involving about 25–30% of total products and components managed in the purchasing portfolio.

The procurement department of Vortice developed a mathematical model, named "Super Index," in order to predict the impact of cost driver fluctuations. The model consists of a cost structure breakdown analysis for the most valuable items included in the bill of materials (BOM) of their products. For each item analyzed (especially components or finished products), Vortice derives primary factors (drivers), which contribute to the expected total cost. These drivers are, for example, raw materials and other components used for the production process, labor, machineries, and industrial overheads. In this analysis, Vortice involves a cross-functional team, with experts from procurement and engineering departments.

Each driver is linked to a commodity index or mixed with other significant indexes (i.e., currencies, labor cost, energy cost, logistics cost). A variation of each index has an impact on expected product cost. Considering the total volume of each product (and some assumptions about product mix not included in the analysis), it is possible to aggregate indexes with a bottom-up construction to estimate the cost of products sold by Vortice. This "Super Index" model makes it easier to simulate variations of cost drivers in order to predict their impact on total spent. A description of the "Super Index" model is described here in Table 2.

As highlighted in the example, the array of values D[x] (the sum is equal to 100) represents the "Super Index." It is possible to apply a variation of each Driver [x] (for simulation, budgeting process) and appreciate the expected change in the percentage of total spending.

The "Super Index" does not consider stocks along supply chains, which are not relevant in terms of volumes. Some suppliers or items' categories can be grouped, with the scope to calculate their weights on the total spent.

3.4 FX Risk Mitigation Strategies

Vortice primarily utilizes contracting and operating strategies for mitigating FX risk in their supply chains (see Table 3), and occasionally employs financial hedging, sometimes in combination with other approaches. *Financial hedging* is considered a viable mitigation approach when cash positions allow, if corporate leadership sees value, and if it complies with the company's general strategy. Financial hedging is adopted by using simple option contracts. The chief financial officer (CFO) runs monthly simulations of the risk exposure related to purchases in foreign currencies.

A significant percentage (60–80%) of the USD risk exposure is covered by using hedging strategies. There is rarely an opportunity to naturally hedge purchases and sales in USD.

Regarding *operating strategies*, the company does not invest in production flexibility, because production plants are specialized in the production of customized products, typically adopting a make-to-stock strategy. Given the need to make long-term forecasts and to control stock levels, forward buying is likewise not used to hedge against FX risk. For the same reasons (i.e., the seasonality of the customer demand, the high level of customization, and the long lead time), Vortice cannot exploit postponement as an FX risk mitigation strategy (Carbonara and Pellegrino 2017).

However, Vortice invests in sourcing flexibility to some extent. There are 50–55 items that can be purchased using alternative suppliers in different currencies, with the main scope of assuring delivery reliability and not only attaining a price advantage. Vortice takes into account the suppliers' risk evaluation and develops a business model with the aim to track risks coming from suppliers' portfolios. Multiple sourcing is an expensive process due to the need for certifying any new supplier. To expedite the certification process of new suppliers, and thus reduce time-to-market for new products, Vortice has invested in their own equipped laboratory. However, it is still a complex and long process and only undertaken when there is evidence the expected savings associated with using the new supplier or the risk reduction offsets the testing and certification costs.

Table 2 A description of the super index model

Supplier	Item	Drv.1	Drv.2	Drv.3	…	Drv.X	Others	Weight
Supp. 1	Item 1	30	20	15	…	5	15	W[1, 1]
Supp. 1	Item 2		40	20	…	…	20	W[1, 2]
…	…	…	…	…	…	…	…	…
∑ Supp. 1						D[x, s]		W[s]
Supp. 2	Item 3	10	15			20	5	
…	…							
Supp. N	Item M		20	10		V[i, x]	30	
…								

Drv.1 … Drv.X are cost drivers (factors) which affect the costs and consequently prices of items bought from suppliers' network
W[s,i] = weight (percentage of total value) of Item [i] purchased from Supplier [s]
V[i,x] = weight (percentage on unit price) of Driver [x] referred to Item [i]
D[x,s] = average incidence of Driver [x] inside portfolio of items bought from Supplier [s]. It is calculated as the sum of products between each couple W[s,i] and V[i,x] extended to each item supplied by Supplier [s]
W[s] = weight (percentage of value) of Supplier [s] compared to total spending value
D[x] = average incidence of Driver [x] on total spending value. It is calculated as the sum of products between each couple W[s] and D[s]

Table 3 Interview highlights on FX Risk mitigation strategies

Themes	Highlights
Financing approaches	"Financial hedging is one of our approaches for FX risk mitigation, which is adopted not each year, but depending on the conditions and the cash available… We use financial hedging for USD, since for the other currencies it is not significant"
Operating approaches	"Vortice doesn't use production flexibility since the production is based on two main aspects. First, a large part of our catalogue is based on products sold from stock. We have a production plant, we need to purchase components 4/5 months before we consume these products in the production (from China), from other countries at least a couple of months before. 95% of items are customised, we don't buy anything from commercial catalogues… The lead time of components is quite long, that means that the flexibility of production is not very high. We cannot decide with a high flexibility margin to switch from one source to another one and change the production plans. The decision to switch the sources is a decision of medium term since we receive components about 4/5 months after the decision is made. For the next 5 months you cannot change anything Second, another problem preventing Vortice from using production flexibility is that in Italy we don't manufacture the same products we produce in China and vice versa" "We have some components (at least 50/55 items) where we have more than one potential supplier. It is not easy to have many alternative suppliers because it is an expensive process. A large part of our process is certified by third parties. To expedite the validation process, we invested in an equipped laboratory, and now we have an internal certified laboratory in order to reduce the lead time (if you go to external laboratory, it takes a longer time). However, we cannot simply switch to another supplier if there are good opportunities in terms of price. We need to repeat a large part of the certification process, which is expensive. Tests may cost from 2000 up to 5000 €, or more. This increases the savings we need to get in order to compensate for this large expense we have at an organizational level. The typical question is: does the saving or the reduction of risk we expect from not having just a sole source compensate for the original costs of multiple sourcing? If yes, we go on with the process, this occurs at the moment for a few components. Our choice to introduce a new supplier is not referred to price opportunities but the most important decision is linked to the reduction of the risk We have few suppliers where we can apply the flexibility referred to only the price, we have to include the risk in the final decision" "As it happens for production flexibility, I cannot decide to wait for a better time to decide if buy or not, we don't have a better time. We need to stick to the production plan, due to the seasonality of products, we need to fulfil the customer in a specific period. Also, customization is for 90% of components which are purchased"

(continued)

Table 3 (continued)

Themes	Highlights
Contracting approaches	"Escalation clauses is another opportunity that we use. Suppliers offering the price in local or other currencies also indicate in the offer the level of FX rate. In some cases, the suppliers indicate a range of variation for FX within which you don't need to adjust price. If they are in the condition to renegotiate price since the fluctuating FX rate penalizes their business, they ask this, and also the opposite. We don't have a fixed frequency to update price. In case the price review is referred to other factors included in the "Super Indice" (labor, commodity, etc.) which drive the business, in that case we fix a frequency to revise the price (typically 6 months). In case of Escalation clause, the main problem is not to sign the contract, but to manage it, since after signing the contract we completely forgot about that. In our ERP we have a managing contract system: each contract has an owner (that typically is the buyer that follows that supplier); there is an alert to revise the price for the buyer and he manages the contract in a proactive way" "Payment term is part of negotiations. Starting from the point that we need to renegotiate the price since the FX rate is out of control, we put a second option on the negotiation table. When I should agree with my supplier on an increment of the price of about 10%, for example, I could make a different proposal, that is a lower increment of price (e.g. 5%) and a reduction of the payment terms in order to compensate for the profit/loss the supplier has due to FX rate fluctuation… we can check profit and loss, balance sheet etc. for Italian suppliers; hence, Vortice knows their cash situation and how much they can be sensible to this kind of proposal, that is, if the payment terms can be leveraged or not. With foreign suppliers it is difficult to collect information about their financial situation. Also, in Europe the info you can gather is few; sometimes you have liabilities, total assets, but you don't have the situation of cash. In such cases, the only way to know it is to visit the supplier and its production plant, check the stock, have a look at the level of saturation of production. In that case, you can discover if reducing the payment terms may be useful for the supplier" "During the last years in EU and in Italy the payment duration is not a significant part of the negotiation, due to the standardization of the payment duration. There is a regulation that rules the maximum payment terms, hence you cannot negotiate different payment terms. You need to sign a contract when both parties agree to change the payment terms provided by law, otherwise the risk is that suppliers can ask you to pay the financial interest if you don't have a document where they agree in writing to a different duration of payment. For this reason, the opportunity to use this option is smaller than in the past. Also, since we don't have long payment duration as in the past, we cannot also exploit the flexibility to anticipate the payment terms within the allowed time windows in order to exploit favourable FX conditions. In such short period, we don't have such significant fluctuations of price that make this option feasible" "We use budget for contingency to hedge against FX risk in case of new product development… we don't only need to buy production components but also moulds… we bought 60–70% of moulds from China. In such cases, at the beginning of the project, also because we have a budget for moulds and equipment, because a large part of the budget is in USD dollars, we can consider taking part of the cash to cover this risk, also because the level of investment is not stable, it depends on the year"

Table 4 Effects of FX variations on final product price

	Supplier purchases (in USD)	Supplier production costs and price (in GBP)		Vortice expectation
Time 1	FX (GBP-USD)=0,68	FX (GBP-Euro)=0,75	gross margin=30% raw material costs=40% labor costs=20% overhead=10% ⬇ Motor unit price= 133,33 GBP	Motor unit price= 133,33 GBP
Time 2 (2 years later)	FX (GBP-USD)=0,75 Raw materials price increase=5% Overhead cost decreases = 3% (lower energy costs)	FX (GBP-Euro)=0,90 **(17% of increase)**	gross margin=30% (equal) **raw material costs=46,32%** labor costs=20% (equal) **overhead=9,7%** ⬇ **Price proposed by the supplier=** **106,02 GBP (117,8 Euro)**	Vortice's expectation is to get a motor unit price reduction of 17% = ⬇ **Price expected by Vortice=** **111,11 Euro**

Vortice's approach to *contracting approaches* aims to create flexibility for creating financial value in various external environmental contexts and situations, as well as for its bargaining power with suppliers. In the case of some customized products, for example, where Vortice is recognized as a market leader, there is consequently power in the contract negotiation.

As a result, the mathematical indexes utilized, which correlate transaction prices with FX rates and/or other drivers costs, are typically used where the advantage coming from a direct negotiation is considered marginal by Vortice's procurement team.

A price revision mechanism linked to the FX rate expresses the risk of the supplier's organization to obtain lower revenues because of FX fluctuation, or the risk of the buyer from price increases due to unfavorable currency rates. Frequently such price revision mechanisms originate from suppliers because the suppliers usually initiate contractual terms, including all commercial ones. Vortice then negotiates starting from the proposal received from the supplier. A more complete approach to negotiation requires a contextual verification of all the other cost factors which contribute to forming the final price, including those connected with other currencies. An example is provided below of the approach Vortice utilizes when there is an adequate set of information available (see also Table 4).

> Vortice buys from UK supplier a motor fan at the unit price of 133,33 EURO. The price was formulated when the FX rate between the GBP and EURO was 0,75. The unit revenue for the supplier is 100 GBP. The supplier has a gross margin of 30%, raw materials costs of 40%, 20% labor costs, and 10% attributed to machining. The supplier purchases raw materials in USD. The FX exchange rate is 0,68 GBP to one USD. After almost two years the FX GBP/EURO has moved from 0,75 to 0,90. This FX rate shift would warrant Vortice requesting a price revision. Vortice's expectation is to attain a price reduction from 133,33 to 111,11 EURO, almost 17% less.
>
> Other factors can likewise trigger a price change request. For example, raw materials cost increases 5% (USD), while the machining cost decreases 3% due to lower energy costs. At the same time labor costs are stable. Furthermore, the FX rate GBP to USD shifts from 0,68 to 0,75. Because of an increment in raw materials and variation in the FX rate GBP/USD the cost has moved from 40 to 46,32 (+15%), labor costs are still 20% and machining costs have moved from 10% to 9,7%. Keeping the same gross margin, the final price is 106,02

GBP. The price proposed in EURO should be 117,8, which is 12% lower than the previous price (133,33) but 6% higher than previous expectations.

Although the use of escalation clauses tied to indices provides Vortice with an opportunity to mitigate FX risks, payment terms and payment duration are not perceived by Vortice as viable FX mitigation approaches. Recently, the EU (hence Italy) created regulations governing payment terms (Italian Decree Law No. 192/2012 and EU 2011/7) by establishing, for instance, the maximum payment duration, which can be negotiated but only according to strict rules (it requires an explicit agreement, genuinely signed voluntarily by both parties, in order to exceed payment terms indicated by law, excluding public companies which cannot exceed such terms). Also, having payment durations shorter than in the past and the ability to anticipate the payment terms within the allowed timeframes mean it has become unfeasible to gain from favorable FX conditions in this context. Further, during such short periods there are usually no significant fluctuations.

Overall, sourcing flexibility and escalation clauses are the two approaches most frequently utilized at Vortice. Sourcing flexibility can be adopted when there are enough suppliers to apply this flexibility approach and as well can be combined with escalation clauses. Vortice's purchasing department prefers, when possible, adopting sourcing flexibility due to the potential value the information obtained through multiple suppliers may have either for improving current relationships or for negotiating with new suppliers. Contrarily, once an escalation contract is signed, the clauses included only require checking the FX price movements and updating the price when needed. The information gathered through multiple sourcing may strengthen the purchasing power of Vortice in negotiating with other suppliers. Escalation clauses are, however, an efficient way to manage contract in different currencies, because establishing rules at the very beginning creates efficiency and limits opportunistic behaviors. In this sense, Vortice perceives sourcing flexibility as a "strategic tool" to adopt from a longer-term perspective (approximately 24 months), based on the FX rate forecasts, while escalation clauses are a "tactical tool" to manage with specific suppliers for shorter-term periodic FX rate fluctuations.

3.5 The Role of Functional Involvement

The collaboration among different functions has been highlighted by Vortice as a key driver in creating and pursuing FX risk mitigation strategies, as summarized in Table 3. Finance takes decisions regarding financial hedging strategies and is strongly integrated with the purchasing and accounting offices, which develop FX risk forecasts and cost analysis. The legal office also serves a significant role in mitigating FX risk, particularly regarding the definition of contracting strategies among different countries. Finance and Legal functions are therefore involved in an integrated decision-making process with the scope to select the proper mix of FX risk mitigation strategies in an efficient and effective manner.

Table 5 Interview highlights on functional involvement

Themes	Highlights
Functional involvement and financial hedging	"For the financial hedging it is the FINANCE function that takes the leadership; PURCHASING and ACCOUNTING are involved to some extent, and FREIGHT FORWARDERS. When we receive invoices from the forwarder, the FX rate is not the real FX rate of the period, since it is fixed by the shipowner for the next incoming weeks, not referred to official sources (such as BCE or others). Vortice spends a lot of money on transportation"
Functional involvement and sourcing flexibility	"LOGISTICS because there is a trade-off where we try to push an extra stock compared to natural requirement of the production plan. As inventory is one of the KPIs of logistic function, we need to negotiate this internally. FINANCE: we have a very good level of cash, but this creates some wrong behaviour, because if you are confident that you have no problem with cash, we can take the wrong decision. We decided to size an ideal working capital for our company business and a physiological cash level. Whatever exceeds a certain size is moved to another account, not an operative one. That means that we cannot buy 1 million motors in USD because there is a big opportunity in terms of FX rate since this decision may create problems for finance"
Functional involvement and escalation clauses	"PURCHASING and only sometimes LEGAL office. Vortice does not have an internal legal office. We have several types of contracts that we use as a template for preparing agreements (we have to adjust parts of them). We submit contracts to the external legal office only when we have important clauses or the first time we sign a new contract different from the past ones"

Those functions that are directly responsible for managing FX risks are purchasing and engineering departments which cooperate in understanding the effects of contract negotiations on the Vortice supply chain and together develop the mathematical models for addressing how FX risk can influence the total cost of products. Vortice highlights the fact that the competitive intensity of the sector requires cross-functional collaboration for mitigating risks related to the supply chain. Information sharing among different departments is also perceived to be essential in order to take better risk management decisions. Vortice recognizes that functional involvement and a high level of expertise in managing and mitigating the various components of global supply chain risk, such as FX risk, may have a direct effect on the organization's financial performance (Table 5).

4 Conclusions

This chapter presents a case study of a multinational SME operating globally in the ventilation systems industry. FX risk is one form of risk many firms are exposed to in their supply chains. Although FX risk exposure has been a challenge for many firms, especially with the increasing pace of global sourcing, our understanding of supply chain strategies for mitigating this form of risk is limited. Supply chain professionals need to consider the financial effects of FX risk from multiple facets, including its impact on production cost variability, as well as understanding the implications in terms of transfer pricing and taxation.

Specifically, the case study of Vortice highlights how FX risk is perceived and managed in a global supply chain where large-sized suppliers sell their products in USD, commercial trade is typically performed in GBP and EURO, and competition is driven by efficiency, low inventory, and servitization. In this industry, like in many others, FX risk has a relevant impact on the total cost of low-margin products. This case provides insights into financing, operating, and contracting strategies firms may want to consider in mitigating FX risk, and how these approaches are selected and adopted in response to volatile currency fluctuations in global sourcing.

Further, FX risk is a cross-functional and cross-organizational challenge. Business professionals in the areas of finance, operations, marketing, and legal, among others, have insights and perspectives of global sourcing practices which can provide a more holistic understanding to alternative approaches firms can adopt in mitigating the effects of FX. Several of these approaches, such as those described in contracting and operating strategies, also require input and coordination with key stakeholders in the supply chain—specifically suppliers and customers. Managers need to understand different financial, operational, and supply chain dynamics from these varying perspectives to select the best choice of risk mitigation strategies.

Vortice considers FX risk as a potential source of higher costs and lower business margins, which can make it more difficult to invest in new products. Given this financial challenge, key mitigation strategies adopted by Vortice are sourcing flexibility and escalation clauses, with financial hedging approaches selectively utilized, as described in the case. Findings from this case can provide firms with an example of approaches beyond financial hedging instruments for addressing FX risk in their global sourcing practices.

Global sourcing has inherent risks from numerous sources. As long as countries and regions retain their respective currencies, the challenge of FX risk exposure will remain. Although many firms have sought to mitigate FX risk utilizing financial hedging, other approaches from a supply chain management perspective can also be considered for adoption. Although this case provides insight as to what one SME does to mitigate this form of risk, much more research is needed to gain an understanding of the contextual factors influencing which approaches are appropriate to adopt and how those approaches can reduce the detrimental financial impact FX risk has on firms.

References

Aggarwal, R., & Goodell, J. W. (2009). Markets and institutions in financial intermediation: National characteristics as determinants. *Journal of Banking & Finance, 33*(10), 1770–1780.

Bandaly, D., Satir, A., & Shanker, L. (2014). Integrated supply chain risk management via operational methods and financial instruments. *International Journal of Production Research, 52*(7), 2007–2025.

Blackhurst, J., Craighead, C. W., Elkins, D., & Handfield, R. B. (2005). An empirically derived agenda of critical research issues for managing supply-chain disruptions. *International Journal of Production Research, 43*(19), 4067–4081.

Brown, G. W. (2001). Managing foreign exchange risk with derivatives. *Journal of Financial Economics, 60*(2), 401–448.

Burnside, C. (2012). Carry trades and risk. In J. James, I. Marsh, & L. Sarno (Eds.), *Handbook of exchange rates* (pp. 283–312). Hoboken: Wiley.

Caniato, F., Gelsomino, L. M., Perego, A., & Ronchi, S. (2016). Does finance solve the supply chain financing problem? *Supply Chain Management: An International Journal, 21*(5), 534–549.

Carbonara, N., & Pellegrino, R. (2017). Real options approach to evaluate postponement as supply chain disruptions mitigation strategy. *International Journal of Production Research*, 1–23. https://ww.andfonline.om/oi/bs/0.080/0207543.017.403663.

Chong, L. L., Chang, X. J., & Tan, S. H. (2014). Determinants of corporate foreign exchange risk hedging. *Managerial Finance, 40*(2), 176–188.

Dufey, G., & Srinivasulu, S. L. (1983). The case for corporate management of foreign exchange risk. *Financial Management, 12*(4), 54–62.

Jia, F., & Zsidisin, G. A. (2014). Supply relational risk: What role does guanxi play? *Journal of Business Logistics, 35*(3), 259–267.

Yang, B., & Yang, Y. (2010). Postponement in supply chain risk management: A complexity perspective. *International Journal of Production Research, 48*(7), 1901–1912.

Zsidisin, G. A., & Gaudenzi, B. (2018). Transcending beyond finance for managing foreign exchange risk. In K. J. Engemann (Ed.), *Routledge companion to risk, crisis and security in business* (pp. 319–327). UK: Routledge.

Zsidisin, G. A., & Wagner, S. M. (2010). Do perceptions become reality? the moderating role of supply chain resiliency on disruption occurrence. *Journal of Business Logistics, 31*(2), 1–20.

Chapter 24
The Paradox of Risk Management: A Supply Management Practice Perspective

Sudipa Sarker

1 Introduction

Theoretically, the risk management process, regardless of its domain of application, consists of at least three linear steps: risk identification, risk assessment and risk mitigation (Purdy 2010; Sodhi et al. 2012). A key assumption here is that a team of people will first identify all the plausible risks by generating a process map of the supply chain or consulting a risk register. Next, these identified risks will undergo a suitable assessment method. Lastly, based on the prioritized values of these risks or assessment scores, suitable measures will be taken. This implicit assumption provides a holistic, single-level and time-independent view of the risk management process, which unfortunately is hardly ever challenged. This is probably because, with a few exceptions (Norrman and Jansson 2004; Ellegaard 2008; Kayis and Karningsih 2012), not many studies in the area of supply chain risk management focus on how the identification, assessment and management of risks are actually carried out inside an organization.

This paper is based on the serendipitous findings from a leading global organization, in which the risk management practice did not match the above portrayal of risk management in the theory (Ho et al. 2015) and widely referred to standards (ISO 2009). To reveal this anomaly between theory and practice, the principal research questions explored in this study are: (1) how are risks managed (i.e., identified, assessed and mitigated) inside a large global organization and (2) why may risk management in practice differ from the theory and widely accepted standards?

To delimit the scope of this paper, the focus is on supply risk management. The rationale behind this delimitation is the seminal paper by Tang (2006), in which the author conceptualizes four basic approaches to supply chain risk management:

S. Sarker (✉)
Department of Industrial and Production Engineering, Bangladesh University of Engineering and Technology, 1000 Dhaka, Bangladesh
e-mail: sudipa@ipe.buet.ac.bd

G. A. Zsidisin and M. Henke (eds.), *Revisiting Supply Chain Risk*, Springer Series in Supply Chain Management 7, https://doi.org/10.1007/978-3-030-03813-7_24

supply management, product management, information management and demand management. This paper stresses the supply management approach to managing supply chain risks. Furthermore, to reveal the paradox and to form an alternative conceptualization of risk management, Whetten's (1989) framework for theoretical contributions is applied. This forms the basis for the key contribution of this paper, which is the assertion that risk management in practice is not as holistic, single-level and time-independent activity as it is presumed to be in theory (Ho et al. 2015) and is widely referred to standards (ISO 2009). Thus, the hope is that this paper will assist researchers in supply chain risk management to develop models that are much closer to reality. Moreover, this paper is expected to enable practitioners to recognize the risk management activities that are carried out within a particular process (e.g., supply management) in a large global organization. This understanding will guide managers towards a more comprehensive picture of supply risk as well as its identification, assessment and mitigation methods. The rest of the chapter is organized in the following sections: literature review, research design, results, discussion, conclusions and future directions.

2 Supply Management Process

The terms "purchasing", "sourcing" and "supply management" are used interchangeably in the literature. However, supply management, in addition to conventional procurement activities, such as searching for and selecting suppliers, order allocation and payment, involves activities such as strategic sourcing and the receiving and inspection of delivered goods (Fraser et al. 2011). According to Tang (2006), supply management deals with five interrelated issues: (1) supply network design; (2) supplier relationship; (3) supplier selection; (4) supplier order allocation and (5) supply contract. For all these issues, certain activities are performed to manage and ensure the supply of incoming materials. For instance, supplier networks can be redesigned by performing activities such as altering the available suppliers and manufacturing facilities. Similarly, supplier relationships can be nurtured by segmenting suppliers into different segments and then deploying strategies for each segment. In supplier selection, the typical activities performed are identifying supplier selection criteria, finding suppliers and selecting suppliers. In this paper, the supply management process of the case organization is examined by scrutinizing four critical activities that are carried out to manage the supply: new supplier selection, strategic sourcing, delivery and inspection and managing the portfolio of existing suppliers.

3 Supply Risk Management

The two predominant sources of supply risks are *inbound supplier failures* and *failures occurring in the supply market* (Zsidisin 2003). *Inbound supplier* refers to a supplier that belongs to the upstream part of the supply chain. Similar to supply chain risk management, the management of supply risk passes through the stages of risk identification, assessment and mitigation (Ho et al. 2015). The difference is that supply chain risk, contrary to and in addition to supply risk, encompasses operational risk and demand risk (Manuj and Mentzer 2008). In this paper, only supply risk management activities that are performed during the supply management process are recognized. Four critical risks from upstream suppliers are identified: financial risk, sourcing risk, performance risk and sustainability risk. The following subsections extract from the literature the key methods for risk identification, assessment and mitigation for managing supply chain risk.

3.1 Risk Identification

The methods for identifying risks are classified into four different categories: common listing, taxonomy-based, scenario-based and objective-based process mapping (Singhal et al. 2011). The common listing approach (Christopher et al. 2003) lists the historical events of risks. In comparison, the taxonomy-based approach (Lockamy and McCormack 2012) provides a framework to extract and organize risk identification activities from business functions. Scenario analysis (Dani and Ranganathan 2008), on the contrary, analyses the key risk factors and their effects on supply chain performance. In addition to identifying risk and creating a risk profile for an organization, the scenario analysis approach assists in building contingency plans for treating various risks. Process mapping, such as process failure mode and effect analysis (PFMEA) (Canbolat et al. 2007) and hazard and operability analysis (HAZOP) (Tummala and Schoenherr 2011), as opposed to the previous approaches, displays the root causes of failures due to risk exposure. Most of these risk identification methods share the holistic assumption of risk management and attempt to recognize all possible risks an organization may have.

3.2 Risk Assessment

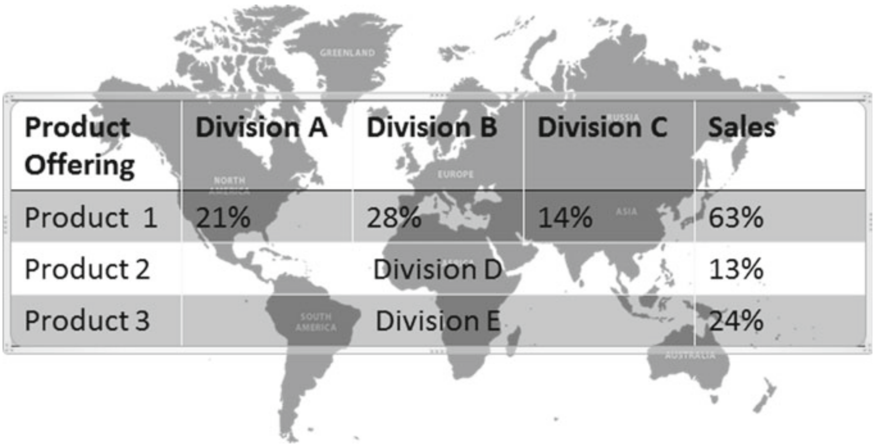
The assessment of supply risk has received much more attention than that of risk identification (Ho et al. 2015). The prevalent risk assessment methods in the literature are the risk matrix (Griffis and Whipple 2012), the analytical hierarchy process (AHP) (Radivojević and Gajović 2014), scenario analysis (Asbjørnslett 2008), different types of FMEA (failure mode effect analysis) (Kumar et al. 2013), frequency space (Ganguly and Guin 2011), multi-criteria scoring (Lockamy and McCormack 2012), the risk pyramid (Tummala and Schoenherr 2011) and so on. Few authors have combined both identification and assessment methods of risk. For instance, Cagliano et al. (2012) have developed a methodology for supply chain risk identification and analysis. Though the above-mentioned techniques are different, they as well share the holistic assumption of risk management and try to assess all possible risks an organization may have using one particular method.

3.3 Risk Mitigation or Treatment

Like risk assessment, risk mitigation has also received significant attention from scholars (Ho et al. 2015). Supply risk can be treated by adopting behaviour-based management techniques (Zsidisin and Ellram 2003), by creating strategic supplier relationships (Hallikas et al. 2005), by reducing the supply base complexity (Choi and Krause 2006), by determining the optimum number of suppliers (Ruiz-Torres and Mahmoodi 2007) and by choosing dual sources instead of single sources (Li et al. 2010). Furthermore, a few authors, in addition to Tang (2006), argue for the criticality of the supply management process for the management of supply risk. For instance, Gualandris and Kalchschmidt (2014) introduce the concept of risk management preparedness and claim that the preparedness of supply chain risk management depends on factors such as supplier integration and development, strategic sourcing, supplier selection, supplier portfolio management and manufacturing postponement. Similarly, Reuter et al. (2010) argue that supplier risk management must be tightly interlocked with the supplier management process.

4 Case Study Methodology and the Single-Case Design

To understand risk management from the supply management practice perspective and answer the research questions, this paper uses a single, in-depth, embedded case study design with the supply management process as the unit of analysis (Yin 2009). A single-case study design is chosen because of its ability to provide a rich as well as a deep understanding of the complexity of the reality (Benbasat 1987). Although single-case studies are rare, they are not entirely absent from the extant literature on supply chain risk management. A few notable ones are those by Norrman and Jansson (2004), Ritchie and Brindley (2007) and Ghadge et al. (2012). Among these studies, only that by Norrman and Jansson (2004) looks closely into the empirical case of Ericsson and presents in detail Ericsson's method of managing supply chain risk. This paper, in comparison with Norrman and Jansson's (2004) study, dives deeply into the risk management activities within the supply management process of a large global organization.



Product Offering	Division A	Division B	Division C	Sales
Product 1	21%	28%	14%	63%
Product 2	Division D			13%
Product 3	Division E			24%

Fig. 1 Case organization's global presence and sales mix

4.1 Empirical Setting

The case organization is a conglomerate of 200 independent subsidiary companies (i.e., business units) spread across 70 countries around the world. Since its inception in 1994, by growing inorganically through acquisitions, the case organization has developed from a regional company into an international group with a current sales value of 7 billion euros and 43,000 employees. The principal product historically has been automatic and manual door locks (product 1). Over the years, the group has diverged into products such as electronic ID and access cards (product 2) and entrance solutions (product 3) to facilities such as hospitals, stadiums and hotels. To manage the diverse as well as dispersed business units, a decentralized management structure is adopted by the top management of the group. As a result, three regional divisions and two global product divisions work independently to manage the business units under each division. A comparative picture of these five divisions is presented in Fig. 1. Divisions A, B and C manufacture and sell product 1 and are located in America, Europe–Africa–Middle East and Asia Pacific, respectively. Divisions D and E operate globally and sell product 2 and product 3, respectively.

4.2 Data Sources

To ensure triangulation of information (Eisenhardt and Graebner 2007), data were gathered from three distinct sources: (1) semi-structured interviews, meetings and discussions with multiple respondents; (2) internal documents that are not available publicly and (3) observational data obtained during interviews, meetings and discussions.

4.2.1 Semi-structured Interviews, Meetings and Discussions

Eighteen respondents were interviewed from the case organization, positioned at different levels (e.g., three vertical levels, i.e., the group level, divisional level and business unit level and five horizontal levels, i.e., five divisions). The chief technology officer, the group supply chain director, the group quality and sustainability manager and the group risk insurance manager were from the group level. Sourcing directors and category managers were from the five divisions of the case organization and represented the divisional level. Purchasing managers represented the business unit level. Most of the respondents from the case organization were met multiple times during interviews, meetings and discussions held over a period of eight months. Additionally, one respondent from a key supplier and two respondents from the insurance provider of the case organization were interviewed to gather information about supply risk management from all the relevant sources.

4.2.2 Documents

The respondents were asked to provide presentations, Excel sheets, risk reports and audit reports. A total of 48 risk-related documents were collected from the organization. The documents included information on supplier criticality assessments, supplier risk assessments, manufacturing site risk assessments, sustainability audit reports, presentations on the case organization's risk management strategies, supply chain failures and sourcing strategies.

4.2.3 Observational Data

The observational data consisted of actual notes from interviews, meetings, discussions and a factory visit. During the factory visit, the author spent an entire day with a purchasing manager of the case organization to scrutinize in detail the risk management activities performed during the supply management process at the business unit level.

4.3 Data Analysis

The data analysis is performed based on the framework questions proposed by David Whetten (1989) for evaluating theoretical contributions. According to Whetten (1989), a complete theory has to have certain key elements, which can be assessed by asking basic questions such as what, who, where and when, how and why. From his perspective, the "what" element is a variable, construct or concept. In this paper, "what" refers to the supply risk of concern. The "who", "where" and "when" elements, in the author's opinion, set the boundary conditions for the theory.

In this paper, "who" refers to the person who manages (i.e., identifies, assesses and mitigates) the risk. The "where" and "when" elements, respectively, refer to the location of the risk and the process in which a particular risk is managed. Although, according to Whetten (1989), the "how" element refers to the mechanisms of relations among the constructs/variables/concepts, in this paper the how element answers the question of how a particular risk is identified, assessed and mitigated. Lastly, the "why" element, according to the author, refers to the underlying factors that explain the relationships between the concepts. Likewise, the why element in this paper refers to the rationale behind a particular method for managing risk in the case organization.

5 Supply Management Process in the Case Organization

Supply management in the case organization is a group-level function. As a result, although the organization is divided into five decentralized divisions, the activities carried out to manage the supply within these five divisions are more or less similar. This subsection is organized according to the critical activities of the supply management process that were discussed in the literature review section as well as being found to be performed in the case organization. These activities are: (1) selection of new suppliers; (2) strategic sourcing; (3) receiving and inspecting goods and (4) managing the portfolio of existing suppliers.

5.1 New Supplier Selection

Supplier selection is considered as one of the key processes for managing the supply of material. The rationales are that the case organization wants to be innovative and cost-efficient and to increase its market presence. Therefore, having new suppliers in the portfolio of existing suppliers is quite important for the organization. According to the procurement director of division B:

… quite frankly, in direct procurement, we have 3400 suppliers at this moment in time; I have put in plan that we will drive down to 1000 by 2020 and of that thousand in 2020, my feeling is 500 will be brand new suppliers.

The above quote projects how critical it is for the case organization to search for new suppliers. The category managers of the case organization were mandated by their respective sourcing directors to select new suppliers. Thus, the new supplier selection is carried out at the divisional level.

5.2 Strategic Sourcing

The term strategic sourcing translates into strategies that are decided at the group level by the group supply chain director. These strategies are to have a limited number of suppliers, strategic partners, supplier agreements, category management, value engineering, a sustainable supply base and zero-defective suppliers (source: company internal presentation). Strategic sourcing, like new supplier selection, is performed at the divisional level. The sourcing directors have the mandate to develop and decide on appropriate sourcing strategies for sourcing key categories of each division. In comparison, the category managers operationalize those strategies and source from the suppliers accordingly. According to the quality and sustainability manager of the group, professional sourcing is about keeping the supplier base limited, choosing strategic partners, managing categories, building supplier relationships, developing suppliers and reducing costs. In his words:

We need a limited number of suppliers and strategic partners … The other thing is the category of management, which is how we organize our categories and sourcing; that is, the glue that contains the supplier relationship, which supplier to develop, how to reduce cost, etc.

5.3 Receiving and Inspecting the Delivered Goods

In the words of a purchasing manager in the case organization, the responsibility of a purchasing manager is as follows:

We are responsible for the supplier base. We do commercial agreements, prices, on-time delivery, frameworks and rules for working with suppliers.

The above quote portrays the types of activities that are performed at the business unit level of the case organization by the purchasing managers. These activities are making agreements with suppliers, setting the prices and ensuring on-time delivery of the purchased items.

5.4 Managing the Portfolio of Existing Suppliers

To manage the portfolio of existing suppliers, one of the key activities performed at the case organization is to carry out sustainability audits. Having a sustainable supply base is a group-level strategy. The group has a corporate KPI for how many suppliers are audited within a year. According to the group's quality and sustainability manager.

Given that it is a sizeable and decentralized organization, shaped by acquisitions, and a growing number of suppliers in low-cost countries, of which some perform manual labour, it is fair to say that the company's supply chain has inherent risks.

The above quote demonstrates the case organization's need to perform sustainability audits on a regular basis because of the growing number of suppliers in low-cost countries with manual labour.

6 Supply Risk Management in the Case Organization

Supply risk management in the case organization is deeply coupled with the supply management processes. At the corporate level, the group has a risk management function. However, this function manages business risks for the case organization. The management procedure for this risk is to transfer the risk to the insurance provider. The properties (e.g., business units) are insured by the insurance provider for risks such as physical damage to the manufacturing units due to fires and natural disasters. However, as an extension of this insurance, and for some rare cases, business units can also be insured for suppliers' failures. All these are evident in the following quote by the group risk insurance manager.

So, there is a risk management process within the group for each division … Our main partner is X, which is also our insurance company, for property and business interaction … Obviously, they target the most profitable and the biggest values (business units), wherever they are. Within the insurance coverage, there is also cover for suppliers and the supply chain, and that goes for as many tiers as you like.

Apart from the business risk, which is managed by the insurance provider of the case organization, four types of risks are observed to be identified, assessed and mitigated across the five supply management processes of the organization. All these risks are mapped according to the Whetten (1989) framework in Table 1 and discussed in the subsequent sections.

6.1 Financial Risk

Financial risk from suppliers is identified, assessed and mitigated during new supplier selection at the divisional level by the category managers. Financial risk refers to the risk of suppliers becoming bankrupt. The identification process of such risk in the case organization is to check suppliers' financial health in a public database named Dun & Bradstreet (D&B). Dun & Bradstreet (D&B) is an organization that holds credit reports on 235 million companies across 200 countries worldwide. By looking at suppliers' financial performance (e.g., payments to suppliers' supplier) over several years, category managers can predict the future bankruptcy risk from suppliers. The mitigation process of such risk is as simple as not selecting or not including a financially unstable supplier as a new supplier to the group. The reason for this risk being identified, assessed and mitigated at the divisional level and by the category managers is that category managers are the ones who are responsible for

Table 1 Risk management within the supply management process

Risks (what?)	Whetten's (1989) Framework	Identification	Assessment	Mitigation
Financial risk	Who?	Category managers		
	When, where?	During new supplier selection, at the divisional level		
	How?	D&B database		Not selecting a financially risky supplier
	Why?	Category managers are in charge of selecting a new supplier in the case organization		
Sourcing risk	Who?	Sourcing directors and category managers		
	When, where?	During sourcing from suppliers, at the divisional level		
	How?	Kraljic matrix, spend analysis		Reducing dependence on suppliers by keeping dual sources and finding alternative materials, etc.
	Why?	Sourcing directors and category managers are responsible for sourcing at the divisional level		
Performance risk	Who?	Purchasing managers		
	When, where?	During delivery and inspection at the business unit level		
	How?	KPIs		Raising quality claims, blacklisting suppliers
	Why?	Purchasing managers deal with contractual issues with the suppliers and receive purchased goods from suppliers		
Sustainability Risk	Who?	Group quality and sustainability manager		
	When, where?	While carrying out sustainability audits at the group level		
	How?	Sustainability audits		Removing suppliers that have high sustainability risks
	Why?	Having a sustainable supply base is a group-level function		

selecting suppliers as well as being entitled to include new suppliers in the existing supply base.

6.2 Sourcing Risk

Sourcing risk from suppliers is identified, assessed and mitigated during the sourcing of materials from the existing portfolio of suppliers at the divisional level by the sourcing directors and the category managers. It includes risks such as volume dependence on suppliers, dependence due to a sole sourcing situation or dependence because suppliers are contract manufacturers and produce customized products only for the case organization. Such risk is identified and assessed in two ways: first, by performing a spend analysis of the purchased goods and material, which gives an indication of how large a volume in monetary values is purchased from a particular supplier and, second, by using matrices such as that of Kraljic (1983), which gives an indication of the supply market of the purchased goods and services. The sourcing risks that are identified and assessed by Kraljic's (1983) matrix are related to the nature of sources (e.g., single source, dual source), the nature of the buyer–supplier power relationship, criticality and the scarcity of the raw material. The mitigation procedures that are followed in the case organization for such risks are to keep dual sources instead of single sources, keep inventories for critical items and redesign the product with an alternative material when its current raw material is scarce. The reason for this risk is identified, assessed and mitigated at the divisional level and by the sourcing directors and category managers, as they are the ones who are responsible for deciding and implementing sourcing strategies for a particular category of materials.

6.3 Performance Risk

Performance risk from suppliers is identified, assessed and mitigated during delivery and inspection of the purchased material, at the business unit level, by the purchasing managers. Risks such as quality risk and delivery risk are considered as performance risk from suppliers. The identification and assessment technique of such a risk is to check it against the key performance indicators (KPIs) for the suppliers. To judge the quality risk from a supplier, the measurement procedure is to count the number of quality complaints raised against it. Similarly, to assess the delivery risk, the number of times that suppliers met the on-time delivery requirement is checked. The mitigation technique for such a risk is to raise quality claims with the supplier and blacklist non-performing suppliers so that no further orders are given to them. The reason for this risk being identified, assessed and mitigated at the business unit level and by the purchasing managers is that the purchasing managers are responsible for receiving and inspecting the materials delivered by the suppliers.

6.4 Sustainability Risk

Sustainability risk from suppliers is identified, assessed and mitigated while carrying out sustainability audits. These audits are driven by the group quality and sustainability manager, who is positioned at the group level. The risks that are considered under the umbrella of sustainability risk from suppliers are ethical concerns, workers' rights, health and safety issues, issues with the working environment and management system and so on. The identification and assessment procedure of such risk is to perform sustainability audits on suppliers from low-cost countries. The mitigation procedure that follows such sustainability audits is to warn non-sustainable suppliers as well as removing suppliers that are high in sustainability risk. The reason for this risk being identified, assessed and mitigated at the group level and by the quality and sustainability manager of the group is that he is responsible for carrying out sustainability audits of low-cost country sources.

7 Discussion

This section of the paper is guided by the research questions for this study. The research questions are: (1) how are risks managed (i.e., identified, assessed and mitigated) inside a large global organization and (2) why may risk management in practice differ from the theory and widely accepted standards?

7.1 How Are Risks Managed (i.e., Identified, Assessed and Mitigated) Inside a Large Global Organization?

The results reveal that various types of risks are identified and assessed using different methods. For instance, financial risk from suppliers is identified and assessed by checking a public credit report database, whereas sustainability risk is identified and assessed by carrying out sustainability audits. For research, this finding implies that methods for risk identification and assessment are required to be customized for the risk in concern. In other words, a method for identifying and assessing financial risk cannot be used for identifying and assessing sustainability risk. Most models in literature for risk identification (e.g., Christopher et al. 2003; Lockamy and McCormack 2012) and assessment (e.g., Ganguly and Guin 2011; Griffis and Whipple 2012) typically attempt to identify and assess all possible risks an organization may have. Possibly because, these models rely on the holistic perception of risk management.

Findings also suggest that for mitigation techniques, the case organization closely follow the prescriptions of literature and vary techniques depending on the type of risk being managed. For example, the mitigation technique for a risk of high-volume dependence on a supplier is to distribute the volume between at least two sources

(Li et al. 2010). In comparison, the mitigation technique for non-performing suppliers is to blacklist them and not to source from them, which is a kind of behaviour-based management (Zsidisin and Ellram 2003) of risk. For research, this implies that when it comes to mitigation techniques, unlike for risk identification and assessment, the practice closely matches the theory.

The findings also reveal that different types of risks are managed at different levels of the organization (e.g., the corporate level, divisional level and business unit level). For instance, financial and sourcing risks are managed at the divisional level, whereas sustainability risk is managed at the corporate level. Moreover, performance risk is managed at the business unit level. Furthermore, the results from the analysis also show that different types of risks are managed by different personnel of the organization. For instance, the sourcing director and category managers manage sourcing-related risk. In comparison, purchasing managers manage quality risk and delivery risk. Similarly, sustainability risk is managed by the group's quality and sustainability manager and financial risk is managed by the category manager. These findings go against the holistic, single-level perception of risk management which is a team of people from several functionalities (e.g., production, marketing and quality) identifies and assesses all plausible risks of an organization and mitigates risks based on the prioritized scores of different risks. For research, these findings imply that in reality different risks can be identified, assessed and mitigated in parallel by several people positioned at various hierarchical levels of an organization. In other words, risk management in practice may not be as integrated as it is presumed in theories.

The outcome of this study also demonstrates that various types of risks are identified, assessed and mitigated during various processes. For instance, financial risk from suppliers is managed during the new supplier selection process, whereas sourcing risk is managed during the sourcing process. Similarly, performance risk is checked only when a supplier is delivering goods to the organization. For research, this implies that various risks may become relevant at different times during the supply management process. In other words, this finding suggests that it may not be possible to identify all possible risks from suppliers during a new supplier selection process because only when the chosen supplier has started delivering goods, can the performance risk from that supplier be recognized.

In sum, the above findings reveal that different types of risks are managed in parallel, at different hierarchical levels of the organization (e.g., divisions, group level and business unit level). The findings consequently question the conventional notion of risk management, which is holistic, single-level, time-independent and thought to be performed by a group of people who identify all the risks so that these risks can be assessed and mitigated. Accordingly, the findings present a fragmented, multilevel and time-dependent view of risk management from the case of a large global organization.

7.2 Why May Risk Management in Practice Differ from the Theory and Widely Accepted Standards?

Based on the results of this paper, this question can have at least three plausible answers. The first is that different risks are owned by different people working at various hierarchical levels of the organization set by the division of labour for managing the supply. Therefore, they manage the risk that they own and use different methods to identify and assess it based on the risk of concern. For instance, because category managers are responsible for new supplier selection, they check the risk (e.g., financial risk) that is relevant for selecting a new supplier. Similarly, a sustainability manager who is responsible for maintaining a sustainable supply base manages the sustainability risk from the supplier. The identification and assessment of this risk are performed while he carries out sustainability audits on suppliers.

The second is that the supply risk is managed during the supply management process and is not managed by a separate risk management function in the organization. This is because, even though the case organization has a risk management function at the corporate level, the risk handled by this function is business-related risk and in this particular case, it is the risk of property damage of the case organization's manufacturing facilities. The management procedure for that risk is to buy insurance from the insurance provider. However, the key question here is whether or not it is possible to manage supply risk within the corporate risk management function. For this particular case, it was not feasible to manage the supply risk within the corporate risk management function because of the nature of the organization.

Consequently, the third plausible answer relates to the structure of the case organization. The case organization is large and operates in 70 countries around the world. It has 200 independent companies under its umbrella, managed by 5 independent and decentralized divisions. Though in every respect, the case organization is one focal firm (e.g., a manufacturing firm) in its supply chain, which consists of numerous suppliers, distributors, wholesalers and customers, it is still not a single organization. To match the diverse supply and customer bases that this particular organization has, the organization needs to be decentralized and dispersed around the globe. This kind of structural diversification of an organization is not new in the organizational theory and design literature and has long been discussed by scholars such as Thompson, March, Simon, Lawrence and Lorsch and termed requisite variety (Dooley 2002). Hence, it is nearly impossible for large and complex organizations to manage supply risk by a group of people at the top level of the organization or by a corporate risk management function. Therefore, risk management activities have to be designated to different people at different hierarchical levels of the organization based on the roles, responsibilities and functions performed.

To summarize, risk management practice may differ from the theoretical assumption of holistic, single-level and time-independent activity because different people may own diverse risks, they may be managing these risks within a particular process (e.g., supply management), and the structure of the organization may create an obstacle for managing risk holistically.

8 Conclusions and Future Research Directions

How are risks managed in organizations? The findings from this paper reveal that risks that arise at different times of a supply management process are managed by different people, working at different levels, using different methods for the identification, assessment and mitigation of risks. The key contribution of this study is this paradoxical view of risk management, which is much more fragmented than is presumed in theories. Conventional risk management theories are anchored in a monolithic view of organizations that is holistic in nature. By using Whetten's (1989) framework for theoretical contributions, this paper discovers that risk in large, global and complex organizations may not be managed by a group of people identifying, assessing and mitigating all types of risks altogether. Moreover, the findings also reveal that not all organizations may manage supply risk as a corporate function. The reality is that risks such as supply risk may be managed within the supply management process of large global organizations. This requires the involvement of different people, because no single individual can manage the whole supply management process. Therefore, the management of such risks has to account for the division of labour, associated diversification of functions, roles and responsibilities as well as the decentralized structure that may exist in large organizations.

Consequently, future models need to be adjusted to this fragmented and silo-based view of risk management. In other words, as necessary as it is to develop models that can identify and assess all risks together, the silo nature of risk management suggests that models to identify and assess a particular type of risk are also required. For instance, models that can predict the financial health of a number of suppliers from a public database or can assess sustainability risk from suppliers. Furthermore, future research should be directed towards understanding why risk management practices in large organizations may occur in silos. Moreover, this paper reveals one (e.g., supply management) of the four approaches to managing supply chain risk by Tang (2006). Future research can also check how supply chain risks are managed by handling the demand, product or information or all of these together.

References

Asbjørnslett, B. E. (2008). Assessing the vulnerability of supply chains. In G. A. Zsidisin & B. Ritchie (Eds.), *Supply chain risk* (pp. 15–33). New York: Springer.

Benbasat, I. (1987). The case research strategy in studies of information systems case research. *MIS Quarterly, 3*(3), 369–386.

Cagliano, A. C., De Marco, A., Grimaldi, S., & Rafele, C. (2012). An integrated approach to supply chain risk analysis. *Journal of Risk Research, 15*(7), 817–840.

Canbolat, Y. B., Gupta, G., Matera, S., & Chelst, K. (2007). Analysing risk in sourcing design and manufacture of components and sub-systems to emerging markets. *International Journal of Production Research, 46*(18), 5145–5164.

Choi, T. Y., & Krause, D. R. (2006). The supply base and its complexity: implications for transaction costs, risks, responsiveness, and innovation. *Journal of Operations Management, 24*(5), 637–652.

Christopher, M., Peck, H., Rutherford, C., & Jüttner, U. (2003). *Understanding supply chain risk: A self-assessment workbook.* Cranfield University: Department for Transport.

Dani, S., & Ranganathan, R. (2008). Agility and supply chain uncertainty: A scenario planning perspective. *International Journal of Agile Systems and Management, 3*(3/4), 178–191.

Dooley, K. (2002). Organizational complexity. In *International encyclopedia of business and management* (pp. 5013–5022).

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: Opportunities and challenges. *Academy of Management Journal, 50*(1), 25–32.

Ellegaard, C. (2008). Supply risk management in a small company perspective. *Supply Chain Management: An International Journal, 13*(6), 425–434.

Fraser, J. P., Leenders, M. R., & Flynn, E. A. (2011). *Purchasing and supply management*. New York: McGraw-Hill.

Ganguly, K. K., & Guin, K. K. (2011). understanding supply risk in supply chain: A fuzzy framework. *International Journal of Logistics Systems and Management, 8*(3), 267–283.

Ghadge, A., Dani, S., & Kalawsky, R. (2012). Supply chain risk management: present and future scope. *International Journal of Logistics Management, 23*(3), 313–339.

Griffis, S. E., & Whipple, J. M. (2012). A comprehensive risk assessment and evaluation model: proposing a risk priority continuum. *Transportation Journal, 51*(4), 428–451.

Gualandris, J., & Kalchschmidt, M. (2014). A model to evaluate upstream vulnerability. *International Journal of Logistics Research and Applications, 17*(3), 249–268.

Hallikas, J., Puumalainen, K., Vesterinen, T., & Virolainen, V.-M. (2005). Risk-based classification of supplier relationships. *Journal of Purchasing & Supply Management, 11*(2–3), 72–82.

Ho, W., Zheng, T., Yildiz, H., & Talluri, S. (2015). Supply chain risk management: A literature review. *International Journal of Production Research, 7543*(September), 1–39.

ISO. (2009). ISO *31000:2009—Risk Management—Principles and Guidelines*, *2009*.

Kayis, B., & Karningsih, P. D. (2012). SCRIS: A knowledge-based system tool for assisting manufacturing organizations in identifying supply chain risks. *Journal of Manufacturing Technology Management, 23*(7), 834–852.

Kraljic, P. (1983). Purchasing must become supply management. *Harvard Business Review, 61*(5), 109–117.

Kumar, S., Boice, B. C., & Shepherd, M. J. (2013). Risk assessment and operational approaches to manage risk in global supply chains. *Transportation Journal, 52*(3), 391–411.

Li, J., Wang, S., & Cheng, T. C. E. (2010). Competition and cooperation in a single-retailer two-supplier supply chain with supply disruption. *International Journal of Production Economics, 124*(1), 137–150.

Lockamy, A. I., & McCormack, K. (2012). Modeling supplier risks using Bayesian networks. *Industrial Management & Data Systems, 112*(2), 313–333.

Manuj, I., & Mentzer, J. T. (2008). Global supply chain risk management strategies. *International Journal of Physical Distribution and Logistics Management, 38*(3), 192–223.

Norrman, A., & Jansson, U. (2004). Ericsson's proactive supply chain risk management approach after a serious sub-supplier accident. *International Journal of Physical Distribution & Logistics Management, 34*(5), 434–456.

Purdy, G. (2010). ISO 31000:2009—Setting a new standard for risk management. *Risk Analysis, 30*(6), 881–886.

Radivojević, G., & Gajović, V. (2014). Supply chain risk modeling by AHP and fuzzy AHP methods. *Journal of Risk Research, 17*(3), 337–352.

Reuter, C., Foerstl, K., Hartmann, E., & Blome, C. (2010). Sustainable global supplier management: the role of dynamic capabilities in achieving competitive advantage. *Journal of Supply Chain Management, 46*(2), 45–63.

Ritchie, B., & Brindley, C. (2007). an emergent framework for supply chain risk management and performance measurement. *The Journal of Operational Reseach Society, 58*(11), 1398–1411.

Ruiz-Torres, A. J., & Mahmoodi, F. (2007). The optimal number of suppliers considering the costs of individual supplier failures. *Omega, 35*(1), 104–115.

Singhal, P., Agarwal, G., & Lal Mittal, M. (2011). Supply chain risk management: review, classification and future research directions. *International Journal of Business Science and Applied Management, 6*(3), 15–42.
Sodhi, M. S., Son, B.-G., & Tang, C. S. (2012). Researchers' perspectives on supply chain risk management. *Production and Operations Management, 21*(1), 1–13.
Tang, C. S. (2006). Perspectives in supply chain risk management. *International Journal of Production Economics, 103*(2), 451–488.
Tummala, R., & Schoenherr, T. (2011). Assessing and managing risks using the supply chain risk management process (SCRMP). *Supply Chain Management: An International Journal, 16*(6), 474–483.
Whetten, D. A. (1989). What constitutes a theoretical contribution? *The Academy of Management Review, 14*(4), 490.
Yin, R. K. (2009). *Case study research: Design and methods* (4th ed.). California: Sage Inc.
Zsidisin, G. A. (2003). A grounded definition of supply Risk. *Journal of Purchasing and Supply Management, 9*(5–6), 217–224.
Zsidisin, G. A., & Ellram, L. M. (2003). An agency theory investigation of supply risk management. *The Journal of Supply Chain Management, 39*(2), 15–27.

Chapter 25
Risk in Complex Supply Chains, Networks and Systems

Christine Mary Harland

1 Introduction

In Harland et al (2003), the supply chain concerns of the time were increasing product and service complexity, e-business, outsourcing and globalisation, all leading to increasingly complex, dynamically changing supply networks, shifting the location of risk within those networks (Harland et al. 2003).

At that time, there had been relatively little research examining networks outside manufacturing. Most supply network research had been from the perspective of a focal organisation trying to influence its upstream supply market and its downstream customer market (Nishiguchi 1994; Womack et al. 1990). In focal firm networks, strong, powerful, focal organisations were attempting to manage risk in the network to reduce their own exposure. However, there are many different types of supply networks; few supply networks are dominated by one, powerful, focal organisation. Some have a number of powerful and influential actors; consider how Nestle, the world's biggest food manufacturer, and Walmart, one of the world's biggest companies and grocers, might exert their own strategies on networks they both operate in. The tensions arising in supply networks from different actors attempting to impose their strategies on the rest of the network is one source of complexity.

In private-sector networks, i.e. those containing mainly for profit organisations, whilst there may be tensions from different actors trying to exert power and control, at least there is goal congruence to some extent; in that, all the actors are seeking to make profits. At a detailed level, it can be argued that there is goal incongruence; in that, each organisation wants to make profit for its own shareholders, so profit distribution across the network is always contested. However, the views and aspirations of all the network players are focused on profit making, providing a degree of commonality of language and culture. Supply networks that contain organisations

C. M. Harland (✉)
Politecnico Di Milano, Milano, Italy
e-mail: christinemary.harland@polimi.it

G. A. Zsidisin and M. Henke (eds.), *Revisiting Supply Chain Risk*, Springer Series in Supply Chain Management 7, https://doi.org/10.1007/978-3-030-03813-7_25

with more extreme goal diversity are more complex for a number of reasons. Consider supply networks in the health sector that contains organisations in public-sector health services, with chains of supply following primary care diagnosis at a general practitioner, to secondary care through referral of a patient to an acute general hospital and possibly to tertiary care to a specialist hospital then to care in the community through social services. These supply networks also contain private-sector care providers, upstream private-sector suppliers of all the equipment and supplies used in healthcare, third-sector organisations providing charitable support, government departments providing funding and political influence and interference, universities integrated with teaching hospitals and so on. In these networks goal diversity of profit making or not for profit, patient care, budget adherence, research excellence, regulatory and legal compliance, political reputation and patient and public voice all form a maelstrom of conflicting objectives, languages, ethics, focus on different time horizons and different styles of governance within the network.

Supply networks that straddle the public–private interface are fascinating, complex networks to research, and to date, there have been very few empirical studies at the level of the network (Provan et al. 2007). Currently we have little understanding of the particular challenges faced by these networks, the risks they face and how they attempt to mitigate those risks. The United Nations and smart cities are examples of supply systems comprising many networks and vast numbers of network actors, with no single organisation able to exercise control over the system. Rather, these are confederal systems with multiple actors with varying degrees of power and influence over their networks.

Conceptualisations of supply risk were focused originally on risk for a single private-sector organisation relating to its immediate suppliers or a supply market failing (Zsidisin 2003). In a study of risks in private-sector supply networks, four types were identified—too low or inappropriate demand, problems in fulfilling customer deliveries, cost management and pricing and weaknesses in resource management and flexibility (Hallikas et al. 2004). However, little attention has been paid, to date, on conceptualisation of supply risk in more complex public- and private-sector networks.

Using examples, this chapter examines issues and challenges facing complex inter-organisational networks and systems that straddle public and private sectors and explore risks and mitigation that are specific to these types of network. These examples are used to form an initial conceptual framework that might be tested in future empirical research.

2 Examples of Complex Supply Networks and Systems

Here three examples are provided to examine risks in complex supply chains, networks and systems where complexity arises from not for profit and private-sector actors interfacing, tensions arising from a number of powerful players being present in the same network and diversity existing in goals, languages, cultures and approaches to governance.

2.1 Example A: Humanitarian Aid Supply

Humanitarian aid supply networks typically involve two main categories of networks—those that respond to crises such as natural disasters, extreme poverty and impact of war or terrorism and those that work in the medium to long term to develop economies, societies and businesses to achieve sustainable improvement. Crisis response networks are driven by the nature of the crisis, the scale and speed of response required and the risk to those affected. Longer term development networks can operate with greater planning and control and more balanced workloads and schedules of resources in the network. This explains why some aid organisations have two main divisions to deal with crisis response and longer term development.

Organisations involved in supplying humanitarian aid come in all shapes and sizes and play a range of roles. Large, United Nations organisations such as UNICEF and the World Health Organization have a particular focus, e.g. improving lives of children or improving health, and they tend to play policy and advisory roles internationally as well as providing aid in response to crises. They require ambidexterity in terms of crisis response and longer term development objectives. Much of their funding comes from the United Nations, but they also run substantial international donation promotions. Other smaller aid organisations rely more heavily on donations, bequests and volunteering to fund and operate their aid networks.

When a disaster or crisis occurs, typically a number of aid organisations will respond, but in addition logistics organisations, private-sector suppliers, individuals, communities local to the crisis, governments and the media will all appear fairly rapidly on the ground at the scene where aid is required. Complex systems of resources have to be mobilised in a crisis. These include:

- cash and tangible donations, such as food, shelter and clothing,
- medical supplies with varying requirements for safety and control,
- organised supply networks of supplies of equipment, staff and consumables internal to the aid organisations,
- munificent private-sector company resources donated,
- individual volunteers,
- military and police force protection,
- local emergency services,
- local governments and communities.

The mobilisation of these resources varies depending on the nature and location of the crisis, the scale and diversity of aid providers and the degree of stakeholder objective diversity.

2.1.1 Nature of the Task

The nature of the crisis brings with it a set of challenges to be faced by the providers of aid. There may be danger for aid providers in territories at war, risk of infection and contagion with epidemics or dangers associated with natural disasters such as flooding after a tsunami.

The geographic location of the crisis impacts on challenges to supply network actors to access those requiring aid, assess the situation, communicate with other actors and local communities, mobilise resources and deliver aid. The demographics of the crisis site impact on challenges to supply network actors—for example, providing aid to a densely populated urban area affected by an earthquake is very different to exploring inaccessible, remote regions to locate communities' cut-off from supplies by civil war.

The scale of the crisis and the speed of impact influence how many aid organisations might respond to provide support. Large-scale devastation that is globally reported by international media triggers response from international aid organisations, individual volunteers, private-sector donors of supplies, public advertising appeals for donations of cash, food and shelter. The larger the scale of the crisis and the greater the speed and severity of impact both influence complexity of supply networks and systems.

2.1.2 Diversity of Actors in the Supply Networks

Large, well established and organised aid providers with a wealth of experience bring with them not only substantial resources but the skills and expertise on mobilisation and coordination of people, materials, information, technology and equipment. They have existing network contacts in local governments and local aid providers that can be activated. This is in stark contrast to the actors who, through goodwill and charity, descend upon a crisis scene volunteering and providing aid where they can. Charitable organisations and benefactors worldwide gather and attempt to distribute donated supplies to the crisis scene. However, keeping the much needed donor and volunteer community on side when they may not have the same level of expertise, skills and understanding of the issues, requires skills on behalf of those actors who step up to act as network leaders.

In a study of emergency aid networks across the EU, it was found that command, control and communication systems of the different actors involved in responding to crises were designed separately and were incompatible. The 24 different official languages and cultures impeded these international aid networks' effectiveness (Casado et al. 2014). The embeddedness of humanitarian aid supply network actors in their own cultural and organisational norms and routines may be more of a constraint to effective coordination than issues of technological integration (Allen et al. 2014). However, technology integration issues can arise where information technologies used by network actors from more developed nations may not gain consensus for use with local actors in less developed nations with poorer infrastructure and less technological awareness (Webersik et al. 2015). Diversity of actors in humanitarian aid supply chains, networks and systems is therefore a significant cause of complexity and resulting challenges.

2.1.3 Diversity of Stakeholder Objectives

Risks arise around conflicting stakeholder and policy objectives; in international aid networks, coordination can be impeded by political interference (Tomasini et al. 2009). International humanitarian aid networks are exposed to greater risk of struggling to gain trust of local populations (Javed et al. 2016) which can lead to misperception and prejudice; local objectives may clash with objectives of the aid providers. The presence of not for profit and for profit organisations in the same aid networks may give rise to conflicting objectives; individual organisations in the network may be unwilling to support improvement of information flows around the network if it involves additional cost to their own organisation (Tomasini et al. 2009).

2.1.4 Risk Mitigation

The level of human resource in humanitarian aid networks is not, in itself, directly related to success or failure of any aid initiative. Rather, it is more about how this is mediated by effective performance of teams in communication, command skills and cross-cultural management (Idris et al. 2014). Recent developments in information technologies, such as social media tools including Facebook and Twitter, and their application in humanitarian aid networks have impacted the coordination mechanisms within these networks. The increased availability and use of mobile phones have enabled reduction of response times to crises (Kabra and Ramesh 2016).

Rather than focusing on an integrated IT solution within the humanitarian aid network, there is recognition that it should be a sociotechnical intervention that integrates with the social, cultural and organisational contexts of the local actors (Haselkorn and Walton 2009). In less developed countries, disasters may be viewed as an 'Act of God', and this may impact the local network actors and communities' preparation for, and response to, crises (Misanya and Øyhus 2015); aid providers have to be prepared to negotiate and motivate potential recipients of aid to be receptive to support.

The emergence of digital volunteering—the use of social media and web technologies to recruit local volunteers—is increasing local empowerment in decision-making in disaster relief (Haworth et al. 2016). In the aftermath of Hurricane Katrina, volunteers used a mobile phone app to register lost and found people (Shankar 2008). Informal networks enabled by volunteers sending texts, images, videos to each other have increased the speed of communication in these complex networks (Keim and Noji 2011; Yates and Paquette 2011). These informal networks complement the more formal mechanisms of international cooperation, such as international collaborative agreements and specifications of satellite tracking systems specific to disaster management (Voigt et al. 2007); this integration has been termed ‘collective knowledge’ (Vivacqua and Borges 2012). Integration of the informal and formal can be seen when informal contributions are coordinated to form a crisis map (Leong et al. 2015). Recent research has specifically addressed the importance of an integrated framework of multiple data sources, formal and informal, for any disaster management situation (Huang et al. 2017). Interaction management is now viewed as being more important than information management to manage risk in humanitarian aid systems (Giordano et al. 2017). Risk mitigation in these networks and systems should be focused on resource orchestration to manage across the diverse actors with conflicting objectives.

In conclusion, humanitarian aid supply chains, networks and systems are complex, and this complexity gives rise to risks that require mitigation that is more reliant on resource orchestration involving social interaction, negotiation and coordination across diverse actors with sometimes conflicting objectives.

2.2 Example 2: Government Procurement

Government spending represents a significant proportion of GDPs internationally, depending largely on the role of the state in the provision of health care, social services and pensions; example percentages of GDP are France (23%), Ukraine (41%), UK (40%) and USA (23%)—see World Bank statistics for the complete world table (World Bank 2016). However, government spending stimulates upstream private and third-sector supply chains that provide materials, products and services to the public sector; the total value of supply to public sectors is estimated to represent between 32 and 57% of gross domestic product of nations when this upstream supply stimulation is taken into account (OECD 2017a). A proportion of government spending is through formal public procurement of goods, services and works by governments and state-owned enterprises; in 2013, governments spent on average of 29% of their total spending through public procurement, ranging from less than 20% in Greece and Portugal to more than 35% in countries such as Estonia, Korea and Japan (OECD 2017a).

Complexity in supply networks and systems associated with government procurement varies depending on the nature of what is being procured, the scale and diversity of procurers and the degree of stakeholder objective diversity.

2.2.1 Nature of the Task

Procuring services from outsourced providers of local government services such as waste management, maintaining street lighting and repairing road damage is fundamentally different to procuring complex defence weapons systems, procuring service and capability to treat a region’s patients at a facility managed acute hospital or procuring police vehicles. Public sectors represent highly complex portfolios of publicly provided services and goods and services that are procured to supply them. In many situations, the task can be distributed and decentralised across a system of government procurement. For example, Government X implemented policies to increase private-sector provision of public services and encouraged all government departments to market test their information systems management. Each government department did this independently, some using a formal government procurement process, others using less formal arrangements directly between IT departments and potential outsourced suppliers. Alarm bells started to ring when it was realised within the central government treasury that 42% of government information systems management contracts had been outsourced, through many independently let contracts, to one supplier from a different country. There was concern that so much control of government information was in the hands of one non-national private-sector company, so brakes were applied by informing all government departments to stop initiating outsourcing with this company. But by this time, there were so many outsourcing contracts going through the system that as the brakes slowed the system down and the outsourcing train came to a halt, more than 70% of the entire national information systems were being managed by one provider that was not based in the same nation as Government X.

2.2.2 Diversity of Actors in the Supply Networks

Some of the government departments who had outsourced their IT to this provider had used a professional procurement process involving specifying clear service-level agreements; others did not have the expertise and capability so had used SLAs provided by the supplier. This gave rise to a wide variety of contract terms, prices and potential for control. The main risks centred around devolved spending and autonomously run government departments with varying motivations and abilities to learn from other departments and share information and political risks associated with growth of private-sector power over government information management.

2.2.3 Diversity of Goals of Supply Network Actors

Public procurement can support and drive the delivery of broader government objectives (Knight et al. 2007); it can play a central role in innovation (Edler and Georghiou 2007; Lember et al. 2011; Uyarra and Flanagan 2010), entrepreneurship (Dennis Jr 2011) and industrial development (Dalpé 1994). Public procurement has been highlighted as a mechanism for delivering social outcomes (McCrudden 2004) and environmental management (Brammer and Walker 2011; Fernández-Viñé et al. 2013; Lee and Klassen 2008). Targeted use of public procurement of public services and construction projects has been successful at improving employment (Erridge 2007). The use of public procurement to favour national suppliers can make a significant economic impact at a national level (Trionfetti 2000). Used strategically, public procurement can promote more competitive supply markets (Caldwell et al. 2005) and can be a significant lever for governments wishing to impact on business, economy and society (Harland et al. 2013). These broader objectives of the strategic use of public procurement vary across government organisations; some have expertise and capability in their public procurement teams to be more strategic, and others are quite operational in how contracts are let. The biggest source of goal diversity occurs at the public–private interface where private, for profit suppliers, engage in public procurement for profit maximisation. Those government departments with capabilities to specify clear service-level agreements may be able to drive their broader government objectives through their outsourced contracts, but using suppliers' SLA templates allows private providers to drive their profit maximisation objectives throughout the life of the outsourced service agreement. In many cases, these less able government departments were locked into 25-year contracts on terms that favoured the supplier.

2.2.4 Risk Mitigation

The devolved nature of government procurement gives rise to challenges of learning across different government departments. Greater collaborative public procurement can improve this learning; collaborative public procurement has been defined as '*the cooperation between two or more public entities in more steps of the procurement process, by bundling their purchasing volumes, exchanging information or sharing resources for obtaining mutual gains*' (Nollet and Beaulieu 2005). Sharing of information and resources across government departments can improve the performance of their procurement (Schotanus et al. 2011). Different organisational forms are required to enable this collaboration; for example, each government department could lead a particular procurement enabling the lead department to develop expertise and resource. Smaller departments or those with less experience of public procurement could 'piggyback' on other departments' contracts (Schotanus and Telgen 2007). Collaborative public procurement can mitigate the power of large, private-sector suppliers (Nollet and Beaulieu 2005).

In conclusion, government procurement can be used strategically to achieve broader government objectives, but the complexity and diversity of how government contracts are let across government departments with devolved spending giving rise to risks of lack of cross-department collaboration and learning.

2.3 Example 3: Healthcare Supply Networks

Health services are challenged with the insatiable appetite of clinicians, patients and the public for the latest technologies and innovations in healthcare treatments in the context of rationed spending in public and insurance led healthcare systems. Spend on health services provision as a proportion of GDP varies internationally, but it is very significant in developed economies (OECD 2017b).

2.3.1 Nature of the Task

Improved quality in healthcare provision depends largely on the uptake and diffusion of innovations (Cutler and McClellan 2001). Within the healthcare sector, innovation can be in many forms such as the provision of new pharmaceuticals, improvement in surgical procedures, development of devices and equipment, patient education and service delivery models (Dixon-Woods et al. 2011). An important source of innovation is from private-sector suppliers to the health service (Brown and Osborne 2012; Hartley 2008). Increasingly ‘open innovation’ is being recognised as an important way of sourcing innovation more widely from broader networks of organisations (Chesbrough 2006; Sawhney and Nambisan 2007). ‘Orchestration’ is a term used increasingly for the coordination of innovation networks (Nambisan and Sawhney 2011). The perception of potential adopters of the innovation and how much they commit to it impacts significantly on whether an innovation will be successfully diffused; adoption has been described as ‘making full use of an innovation as the best course of action available’ (Rogers 2004). Innovations can be adopted as they are adapted to the specific context or rejected. So adoption of an innovation relates to the willingness of organisations or individuals to consider its potential, irrespective of their involvement in its development. The more an innovation is adopted by individuals within an organisation, the greater its value grows as it becomes institutionalised (Nelson et al. 2004). However, the complexity and diversity of the healthcare system impede diffusion of innovation in the practice of healthcare delivery (Fitzgerald et al. 2003); this is where innovation and supply networks and systems overlap.

2.3.2 Diversity of Supply Network Actors

Healthcare supply networks are challenged by the need for ambidexterity as they seek openly for innovations but also have to exploit and diffuse those innovations in highly regulated and controlled environments (Salge et al. 2013). This ambidexterity is more pronounced in health care as it spans the public–private interface through sourcing innovation from private-sector suppliers, but it also spans the public-sector public interface in its engagement of patients and public in diffusion of innovation through supply networks providing innovative healthcare treatments. Rather than the two hands of innovation exploration and exploitation being able to operate simultaneously and equally well, the multiple stakeholders involved in healthcare networks require more octopus-like ambidexterity.

2.3.3 Diversity of Goals of Supply Network Actors

The complexity of networks involving private-sector suppliers, health service providers and patients and the public is contributed to by the extreme diversity of goals of all the stakeholders involved. Actors engaged in innovation and diffusion in health care include clinicians, patients, universities, private-sector suppliers, regulators, commissioners, politicians and professional associations. Mapping these innovation and supply networks requires tracing the various flows around the network of finance, policies, knowledge and care provision in addition to traditional supply network flows of materials, products and services. The diversity of goals can cause conflict and blocking of innovations, so they do not become diffused across supply networks. For example, clinicians have their own research interests that may cause clinical preference to reject innovations. Suppliers may attempt to push profit-maximising innovations over best value solutions. Patients may not have sufficient understanding and capability to accept appropriate innovations; for example, mothers may be reluctant to take medication that could prevent cerebral palsy in pre-term births, and midwives may be reluctant to cause them anxiety by trying to persuade them. General practitioners operating as small businesses may exhibit reluctance to provide anticoagulation medication to prevent stroke in an increasingly costly, ageing population under their care.

Healthcare networks and systems are extremely complex in terms of their tasks, the diversity of actors in the networks and their goal diversity; these complexities give rise to particular risks that require mitigation.

2.3.4 Risks and Their Mitigation

Healthcare systems are complex confederations of organisations and therefore do not operate in the same way as single private-sector organisations with executive boards with clear decision-making structures and power. Rather, policy is often provided as guidance and individual healthcare providing organisations and individuals within them have varying visibility, understanding and motivation to implement guidance. Risks arise around difficulties in permeating established social networks within many different supply networks across the supply system to promote and nurture adoption of proven innovations. Competence trust is an important aspect of innovation diffusion in addition to formal arrangements such as contracts (Li et al. 2010). There is therefore greater need for motivation, promotion, encouragement and persuasion for supply networks to enable scaling up and rolling out of innovations.

Dealing with the extreme ambidexterity requirement, multi-lateral boundary spanning is required to facilitate coordination of diffusion across healthcare supply networks (Patru et al. 2015). This boundary spanning requires leveraging social connections and social capital that resides in networks of individuals and organisations (Leenders and Gabbay 2013).

3 A Synthesis of Risks and Their Mitigation in Complex Supply Networks and Systems

In the three examples provided, there are some commonalities relating to complexity arising from the complex nature of the tasks being performed, the diversity of the actors and goals in these complex networks and systems. This complexity gives rise to particular types of risk that can be categorised as:

- Supply network orchestration risk,
- Supply network learning risk,
- Supply network innovation risk.

Discussion and research around supply, innovation and learning networks have largely been separated traditionally. This may be due in part to greater clarity of the distinctly separate systems in private-sector manufacturing environments where most network research has been performed.

3.1 Supply Network Orchestration Risk

When Airbus orchestrates the network to deliver production scale of a new aircraft, as the focal actor it can ‘conduct’ an established ‘orchestra’ or network comprising known suppliers who are experts with known organisational resource to leverage. Information systems can be integrated across the network. Planning and control can be formalised into work packages that can be coordinated by the orchestrator.

In complex confederal networks, such as the humanitarian aid example, clear, highly planned orchestration is more difficult. Larger actors may attempt to take on this role, but they have to deal with the convergence of many, varied actors, with incompatible information systems, coordination mechanisms, languages, cultures and competences.

Supply network orchestration risk is a particular feature in complex networks and systems that, if realised into loss, can cause delays or failure in product and service provision, confusion in prioritisation of scheduling of supply, waste of resources, imbalances in capacity, conflict amongst network actors and a range of other inefficiencies and reduced effectiveness. In humanitarian aid or healthcare provision, the loss may be mortality or morbidity.

3.2 Supply Network Learning Risk

When the board of Proctor and Gamble decides to benefit from learning across diverse divisions supplying cleaning products and healthcare products to stimulate new ideas combining knowledge from both areas, through executive action it can create a learning environment that facilitates knowledge sharing and learning. Crest Whitestrips and Olay Daily Facials were innovated through learning shared through P&G's Connect and Develop programme. In complex confederal systems, heterogeneity of network actors and range of tasks give rise to particular challenges to learn across organisational boundaries.

Supply network learning risk arises when there is lack of recognition and visibility of other network actors with whom inter-organisational learning might be beneficial. Lack of an executive board in confederal systems hinders executive power to launch and develop learning initiatives. Learning often arises when things go wrong, investigations are made and similarities and potential for learning emerge after the fact; this is often the case in government procurement. Public sectors are exposed to reputational and political risk as private-sector commentators and independent auditors reveal the apparent ridiculousness of 18 brands of surgeons' gloves being purchased within a hospital, all ambulance authorities or state police forces across a nation procuring different designs of ambulance and police vehicles. 'Joined-up government' has been an international mantra, but still there is little evidence of successful collaborative public procurements.

3.3 Supply Network Innovation Risk

Organisational ambidexterity research and practice positions innovation exploration and exploitation as two different activities requiring different skills and resources. The transition from exploration to scaling up to commercial volumes is problematic in single private-sector organisations with executive boards overseeing the two hands of the ambidextrous organisation.

Supply network innovation risk is particularly acute in complex confederal systems. Smart cities have difficulties in scaling up good ideas across municipalities with devolved funding and decision-making. National healthcare systems face frustrating challenges of why tested, approved, value for money innovations in healthcare practice are diffused patchily across the confederal system.

3.4 An Initial Conceptual Framework for Risk in Complex Supply Networks and Systems

The main features that distinguish risk and risk management in complex confederal supply networks and systems from organisational or simpler network risk management are around diversity of tasks, actors and goals. These give rise to particular aspects of complexity in supply, innovation and learning. Risks intrinsic to supply orchestration, innovation diffusion and learning leveraging require mitigation mechanisms and approaches that are distinct from those in simpler settings.

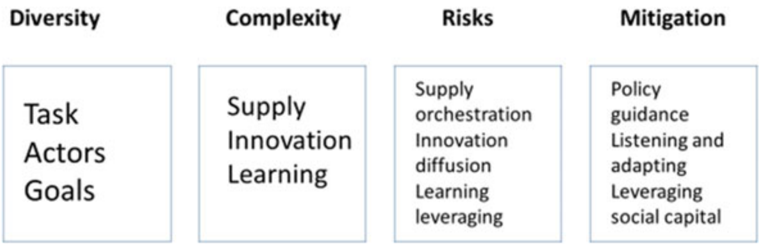


Fig. 1 Risk in complex supply chains, networks and systems: an initial conceptualisation

Softer, people-focused approaches are necessary to exploit the social capital that is the glue in these complex networks and systems (Fig. 1).

4 Reflecting on Theories

Supply chain management research has been overly focused on borrowing two theories from other disciplines, namely transaction cost economics (TCE) and resource-based view of the firm (RBV). To examine issues of risk management in more complex, confederal networks and systems where rational planning and control require complementing with social networking and negotiation, theories based on more rational economic and strategic management thinking are, on their own, insufficient.

To analyse the issues of diversity discussed in the examples provided, principle–agent theory may illuminate the severity of goal incongruence, approaches to risk and information asymmetry. Whilst resource orchestration theory, derived from RBV, and planning and control theories from operations management may be useful lenses to use when these confederal networks and systems are operating in a relatively planned way, when they start to spiral out of control or are never in any sort of control from the outset, other theories are required. Theories such as the Industrial Marketing and Purchasing (IMP—now International Marketing and Purchasing) network theory may inform understanding of how actors cope in networks through managing relationships with immediate network contacts but accepting they cannot manage the network as a whole. Complex adaptive systems theory from biological sciences has been proposed recently as an important theory for supply chain management (Carter et al. 2015) and may help researchers to understand the risks faced by network actors who are constantly adapting to a shifting, changing network. The examples show that risk mitigation is more socially influenced in complex settings, so social capital theory from sociology has been shown to be the glue that holds networks together (Harland et al. 2017). Theories from psychology may help inform how to operate and manage in networks where relational interaction is more important than more systematised operations and information planning and control. Relational theory may aid understanding of how to form and develop successful relationships within complex networks. Expectancy disconfirmation theory, originating from psychology but now used widely in fields relating to provision of information, consumer and government services, may help reveal how risks in complex networks and systems may be mitigated through exposing misperceptions of requirements and performance arising in part from diversity.

5 Summary

Supply chain management research is growing and developing from its origins of understanding relating to private-sector manufacturing supply chains and networks. Consideration of manufacturing and service, private, public and third-sector settings require our understanding of risk and risk management also to grow and develop. Through three examples based on a range of empirical research projects in complex confederal networks and systems, this chapter has tried to reflect on how our examination of supply chain risk has to embrace a wider range of issues and requires new conceptual frameworks and use of a broader set of theories from other disciplines.

References

Allen, D. K., Karanasios, S., & Norman, A. (2014). Information sharing and interoperability: the case of major incident management. *European Journal of Information Systems, 23*(4), 418–432.

Brammer, S., & Walker, H. (2011). Sustainable procurement in the public sector: an international comparative study. *International Journal of Operations & Production Management, 31*(4), 452–476. https://oi.rg/0.108/1443571111119551.

Brown, K., & Osborne, S. P. (2012). *Managing change and innovation in public service organizations*. Oxford: Routledge.

Caldwell, N., Walker, H., Harland, C., Knight, L., Zheng, J., & Wakeley, T. (2005). Promoting competitive markets: The role of public procurement. *Journal of Purchasing and Supply Management, 11*(5), 242–251.

Carter, C. R., Rogers, D. S., & Choi, T. Y. (2015). Toward the theory of the supply chain. *Journal of Supply Chain Management, 51*(2), 89–97.

Casado, R., Rubiera, E., Sacristan, M., Schütte, F., & Peters, R. (2014). Data interoperability software solution for emergency reaction in the Europe Union. *Natural Hazards and Earth System Sciences Discussions, 2,* 6003–6031.

Chesbrough, H. W. (2006). *Open innovation: The new imperative for creating and profiting from technology*. Harvard: Harvard Business Press.

Cutler, D. M., & McClellan, M. (2001). Is technological change in medicine worth it? *Health Affairs, 20*(5), 11–29.

Dalpé, R. (1994). Effects of government procurement on industrial innovation. *Technology in Society, 16*(1), 65–83.

Dennis, W. J., Jr. (2011). Entrepreneurship, small business and public policy levers. *Journal of Small Business Management, 49*(1), 92–106.

Dixon-Woods, M., Amalberti, R., Goodman, S., Bergman, B., & Glasziou, P. (2011). Problems and promises of innovation: Why healthcare needs to rethink its love/hate relationship with the new. *Quality and Safety in Health Care, 20*(Suppl 1), i47–i51.

Edler, J., & Georghiou, L. (2007). Public procurement and innovation-resurrecting the demand side. *Research Policy, 36*(7), 949–963.

Erridge, A. (2007). Public procurement, public value and the Northern Ireland unemployment pilot projec. *Public Administration, 85*(4), 1023–1043. https://oi.rg/0.111/.467-299.007.0674..

Fernández-Viñé, M. B., Gómez-Navarro, T., & Capuz-Rizo, S. F. (2013). Assessment of the public administration tools for the improvement of the eco-efficiency of small and medium sized enterprises. *Journal of Cleaner Production, 47,* 265–273. https://oi.rg/0.016/.clepro.012.8.26.

Fitzgerald, L., Ferlie, E., & Hawkins, C. (2003). Innovation in healthcare: How does credible evidence influence professionals? *Health and Social Care in the Community, 11*(3), 219–228.

Giordano, R., Pagano, A., Pluchinotta, I., del Amo, R. O., Hernandez, S. M., & Lafuente, E. S. (2017). Modelling the complexity of the network of interactions in flood emergency management: The Lorca flash flood case. *Environmental Modelling and Software, 95,* 180–195.

Hallikas, J., Karvonen, I., Pulkkinen, U., Virolainen, V.-M., & Tuominen, M. (2004). Risk management processes in supplier networks. *International Journal of Production Economics, 90*(1), 47–58.

Harland, C., Brenchley, R., & Walker, H. (2003). Risk in supply networks. *Journal of Purchasing and Supply Management, 9*(2), 51–62.

Harland, C., Telgen, J., & Callender, G. (2013). International research study of public procurement. *The SAGE Handbook of Strategic Supply Management*, 372.

Harland, C. M., Hendy, C., Touboulic, A., & Wang, Y. (2017). Supply network orchestration of social capital in healthcare. In *26th Annual IPSERA Conference, Budapest, Hungary, NEVI Zorg Best Healthcare Paper Award*. ISBN 978-90-823707-1-3.

Hartley, J. (2008). *The innovation landscape for public service organizations*. Cambridge: Cambridge University Press.

Haselkorn, M., & Walton, R. (2009). The role of information and communication in the context of humanitarian service. *IEEE Transactions on Professional Communication, 52*(4), 325–328.

Haworth, B., Whittaker, J., & Bruce, E. (2016). Assessing the application and value of participatory mapping for community bushfire preparation. *Applied Geography, 76,* 115–127.

Huang, Q., Cervone, G., & Zhang, G. (2017). A cloud-enabled automatic disaster analysis system of multi-sourced data streams: An example synthesizing social media, remote sensing and Wikipedia data. *Computers, Environment and Urban Systems, 66,* 23–37.

Idris, A., & Nizam Che Soh, S. (2014). Determinants of HADR mission success: exploring the experience of the Malaysian army. *Disaster Prevention and Management, 23*(4), 455–468.

Javed, S., Afzal, H., Arif, F., & Majeed, A. (2016). Reputation management system for fostering trust in collaborative and cohesive disaster management. *Management, 7*(7).

Kabra, G., & Ramesh, A. (2016). Information technology, mutual trust, flexibility, agility, adaptability: Understanding their linkages and impact on humanitarian supply chain management performance. *Risk, Hazards & Crisis in Public Policy, 7*(2), 79–103.

Keim, M. E., & Noji, E. (2011). Emergent use of social media: a new age of opportunity for disaster resilience. *American journal of disaster medicine, 6*(1), 47–54.

Knight, L., Harland, C., Telgen, J., Thai, K., Callender, G., & McKen, K. (2007). *Public procurement: International cases and commentary*. Oxford: Routledge.

Lee, S. Y., & Klassen, R. D. (2008). Drivers and enablers that foster environmental management capabilities in small-and medium-sized suppliers in supply chains. *Production and Operations Management, 17*(6), 573–586.

Leenders, R. T. A., & Gabbay, S. M. (2013). *Corporate social capital and liability*. Berlin: Springer Science & Business Media.

Lember, V., Kalvet, T., & Kattel, R. (2011). Urban competitiveness and public procurement for innovation. *Urban studies, 48*(7), 1373–1395.

Leong, C. M. L., Pan, S. L., Ractham, P., & Kaewkitipong, L. (2015). ICT-enabled community empowerment in crisis response: Social media in Thailand flooding 2011. *Journal of the Association for Information Systems, 16*(3), 174.

Li, J. J., Poppo, L., & Zhou, K. Z. (2010). Relational mechanisms, formal contracts, and local knowledge acquisition by international subsidiaries. *Strategic Management Journal, 31*(4), 349–370.
McCrudden, C. (2004). Using public procurement to achieve social outcomes. *Natural Resources Forum, 28*(4), 257–267. https://oi.rg/0.111/.477-947.004.0099..
Misanya, D., & Øyhus, A. O. (2015). How communities' perceptions of disasters influence disaster response: Managing landslides on Mount Elgon, Uganda. *Disasters, 39*(2), 389–405.
Nambisan, S., & Sawhney, M. (2011). Orchestration processes in network-centric innovation: Evidence from the field. *The Academy of Management Perspectives, 25*(3), 40–57.
Nelson, R. R., Peterhansl, A., & Sampat, B. (2004). Why and how innovations get adopted: A tale of four models. *Industrial and Corporate Change, 13*(5), 679–699.
Nishiguchi, T. (1994). *Strategic industrial sourcing: The Japanese advantage*: Oxford: Oxford University Press on Demand.
Nollet, J., & Beaulieu, M. (2005). Should an organisation join a purchasing group? *Supply Chain Management: An International Journal, 10*(1), 11–17.
OECD (2017a). General government spending (indicator). https://oi.rg/0.787/31cbf4d-n (Accessed on 20 January 2017).
OECD (2017b). *Health at a glance 2017*. OECD Publishing.
Patru, D., Lauche, K., van Kranenburg, H., & Ziggers, G. W. (2015). Multilateral boundary spanners: creating virtuous cycles in the development of health care networks. *Medical Care Research and Review, 72*(6), 665–686.
Provan, K. G., Fish, A., & Sydow, J. (2007). Interorganizational networks at the network level: A review of the empirical literature on whole networks. *Journal of Management, 33*(3), 479–516.
Rogers, E. (2004). *Diffusion of innovations* (5th ed.). Free press.
Salge, T. O., Farchi, T., Barrett, M. I., & Dopson, S. (2013). When does search openness really matter? A contingency study of health-care innovation projects. *Journal of Product Innovation Management, 30*(4), 659–676.
Sawhney, M., & Nambisan, S. (2007). *The global brain: Your roadmap for innovating faster and smarter in a networked world*. New Jersey: Pearson Prentice Hall.
Schotanus, F., Bakker, E., Walker, H., & Essig, M. (2011). Development of purchasing groups during their life cycle: From infancy to maturity. *Public Administration Review, 71*(2), 265–275.
Schotanus, F., & Telgen, J. (2007). Developing a typology of organisational forms of cooperative purchasing. *Journal of Purchasing and Supply Management, 13*(1), 53–68.
Shankar, K. (2008). Wind, water, and Wi-Fi: New trends in community informatics and disaster management. *The Information Society, 24*(2), 116–120.
Tomasini, R., Van Wassenhove, L., & Van Wassenhove, L. (2009). *Humanitarian logistics*. London: Springer.
Trionfetti, F. (2000). Discriminatory public procurement and international trade. *The World Economy, 23*(1), 57–76.
Uyarra, E., & Flanagan, K. (2010). Understanding the innovation impacts of public procurement. *European Planning Studies, 18*(1), 123–143.
Vivacqua, A. S., & Borges, M. R. (2012). Taking advantage of collective knowledge in emergency response systems. *Journal of Network and Computer Applications, 35*(1), 189–198.
Voigt, S., Kemper, T., Riedlinger, T., Kiefl, R., Scholte, K., & Mehl, H. (2007). Satellite image analysis for disaster and crisis-management support. *IEEE Transactions on Geoscience and Remote Sensing, 45*(6), 1520–1528.
Webersik, C., Gonzalez, J. J., Dugdale, J. A., Munkvold, B. E., & Granmo, O. -C. (2015). *Towards an integrated approach to emergency management: Interdisciplinary challenges for research and practice.*
Womack, J. P., Jones, D. T., & Roos, D. (1990). *Machine that changed the world*. New York: Simon and Schuster.
World Bank (2016). *World bank national accounts data*.

Yates, D., & Paquette, S. (2011). Emergency knowledge management and social media technologies: A case study of the 2010 Haitian earthquake. *International Journal of Information Management, 31*(1), 6–13.

Zsidisin, G. A. (2003). A grounded definition of supply risk. *Journal of Purchasing and Supply Management, 9*(5–6), 217–224.

Chapter 26
Surfing the Tides of Political Tumult: Supply Chain Risk Management in an Age of Governmental Turbulence

Michael E. Smith

1 Introduction

While the dominant focus in discussions of supply chain risk management has been on dyadic relationships, even a very cursory familiarity with global events should serve to make it clear that business interests are profoundly impacted by politics, and the speed and frequency of the shifting political tides are expanding at a pace that is almost unimaginable. In fact, a little reflection should make it clear that businesses face a very different political environment today than they did even a few years ago, and the forms of risk arising in this environment have also become more complicated (Rice and Zegart 2018). Those seeking to manage risk in these tumultuous times need to be aware of geopolitical risk, understand its origins, and be prepared to take effective steps to mitigate risk exposure.

Risk associated with the political policy process has been a standard concern in corporate strategy since the middle 1980s (Keim 2001). Much of the focus in this arena has been from a financial perspective that deals with flows of capital across borders, where levels of risk are monetized, and risk management is substantially addressed in terms of insurance and other instruments of finance (Toksoz 2014). On the other hand, geopolitical risk has not been well represented in the supply chain risk management (SCRM) literature. This is an unfortunate state of affairs, given that in SCRM, the concerns are much more substantial than can be addressed from a purely financial perspective. Success in SCRM incorporates many dimensions, including flows of materials, services, information, and capital, as well as characteristics of the constituents of those flows (e.g., quality, quantity) that often determine both the level of operational and strategic success for the firms in the supply chain. In other words, SCRM, as is well portrayed throughout this book, must deliver responsiveness well

M. E. Smith (✉)
Dean of the School of Management, F. James McDonald Chair of Supply Chain Management, Kettering University, Flint, MI, USA
e-mail: mesmith@kettering.edu

G. A. Zsidisin and M. Henke (eds.), *Revisiting Supply Chain Risk*, Springer Series in Supply Chain Management 7, https://doi.org/10.1007/978-3-030-03813-7_26

beyond a purely financial strategy to be successful. At a time when political changes are reshaping the environment in which global supply chains function, when even countries long perceived as stable markets have recently been subjected to political shifts that create uncertainty in the marketplace (e.g., Ghemawat 2017), it is troubling that there is a lack of sound guidance for scholars and practitioners seeking to manage such supply chain risk.

This chapter provides an overview of political strategy for SCRM and how political competencies can be developed to help organizations deal with the uncertainties inherent in the political turbulence through which SCRM must help organizations navigate. Such turbulence can be conceptualized in three general categories. There is risk that arises through government actions that impact the trade environment (risk engendered by commission of governments and their officials). It is worth noting that typical portrayals of geopolitical risk have generally focused on the role of bad actors in the political arena, often in the form of despots manipulating the trade environment to their advantage. However, in today's trade climate, reality has grown a great deal more complicated than is suggested by this stereotype (Rice and Zegart 2018).

The second source of risk, also rooted in the actions of governments, is the circumstance where the lack or inadequacy of actions results in impact in the trade environment (risk engendered through omission by governments and their officials). An example of such risk arises when a weak government engenders supply chain risk by undermining the rule of law.

The third source of risk arises from actors outside of central governments. Technology has led to an environment that allows individuals and groups to effectively influence organized responses to perceived failings of businesses. For SCRM, this increasingly ubiquitous form of influence can impact a firm even when direct control is not present, because key stakeholders have become increasingly sophisticated in linking firms to the actions of suppliers, even in tiers far removed from immediate control (Wright et al. 2007).

These three sources of risk, acts of government commission, acts of government omission, and political acts of players outside of government, create a challenging environment in which organizations must attempt to identify, understand, and seek to develop responses adequate to managing supply chain risk. The next sections will characterize each of these categories of risk and provide meaningful alternatives for risk management.

2 Supply Chain Risk from Government Actions that Damage the Trade Environment

Geopolitical risk can readily be typified as resulting from the actions of a government in many cases. From this perspective, the potential for damage occurs when the government commits actions that increase the risk in global supply chains, such as when they institute measures protective of domestic business interests as compared with global interests (protectionism), or utilize trade weapons to influence others, such as leveraging scarcity of an important commodity as a tool for influencing the national policy of a trading partner. Recent political events highlight the importance of attention to this type of risk.

Electoral support for the UK to leave the European Union (so-called Brexit) and recent shifts toward nationalistic politics in a number of countries, including the USA, serve to highlight the need for serious examination of supply chain risk with its roots in geopolitical events (Smith 2016). It can readily be argued that the momentum behind Brexit is symptomatic of a broader shift in the political environment reflecting distrust of globalization and a drive toward nationalistic politics seeking sovereignty and independence. The immediate impact of Brexit is to significantly increase the level of uncertainty associated with trade involving the European Union, and specifically, the UK.

It is instructive to note that Brexit represents a negative reaction among the citizens of one nation to a trade agreement. Such agreements are a major tool in global trade that are aimed in part at curbing more immediate and direct disruption of supply chains attributable to political events, such as protectionist measures and measures enacted by one nation to influence another (e.g., China's export ban of rare earth minerals to Japan in 2011–2012; Khanna and Mitachi 2016). The potential for harming global supply chains as a result of such activity was highlighted by the release in 2016 of a report under the auspices of the World Economic Forum entitled "The Age of Economic Coercion: How Geo-politics is Disrupting Supply Chains, Financial Systems, Energy Markets, Trade and the Internet" (Global Agenda Council on Geo-economics 2016). In this report, the authors point out that there is a growing move toward coercive measures instituted by one government against external businesses to influence the actions of other governments. In such cases, business interests are intentionally and directly harmed as an instrument of influence wielded by political interests. Table 1 provides a sampling of measures that governments frequently employ in a coercive manner. The frequency and range of implementation of such measures are increasing rapidly.

Table 1 A partial listing of coercive government measures that can result in supply chain risk

• Full economic blockade/embargo	• Travel/visa bans
• Freezing of financial assets	• Financial sanctions
• Import bans/reductions	• Export bans/reductions
• Tariff increase/tariff discrimination	• Unfavorable taxation
• Increase import/export inspections	• Closing of businesses/expropriation
• Encouraging public boycotts	• Denying regulatory approval/licenses
• Cutting transportation links	• Aid suspension
• Cancelling/interruption of international negotiations/meetings	• Withholding of previously agreed loans, orders, projects

Instead of working to implement open trade, governments are increasingly utilizing global supply chains as weapons against other governments. This is the kind of activity against which trade agreements have been developed in recent history. Movement away from regard for such agreements represents a solid indication that we should anticipate further acceleration of the coercive use of measures that impede effective global supply chains. A particularly alarming reality is that there is likely to be positive feedback as governments react to coercive measures of others, effectively accelerating the trend until such time as the level of harm is so substantial that it brings business interests together to leverage the development of new trade agreements (i.e., when businesses band together to support free trade).

The importance of activities like those listed in Table 1 for SCRM was directly addressed by the authors of the World Economic Forum White Paper, noting that, "For companies, the most alarming question is how geo-economics will affect global supply chains" (Global Agenda Council on Geo-economics 2016, p. 5). In addition to the direct impact of coercive measures imposed by governments, firms need to be aware that the measures they take to adapt to such coercion may also engender negative reactions from stakeholders, damaging firm reputation and potentially spawning stakeholder activities disruptive to the conduct of business (Wright et al. 2007).

3 Omission or Inadequacy of Government Action as a Source of Supply Chain Risk

In the case of risk from inaction or lack of effective action, governments sow risk to global supply chains when they fail to address factors important to trade. Inaction or ineffectiveness that can disrupt trade includes failure to adequately prepare for or address natural disasters or failures to effectively address unrest at the social or political level. Supply chain risk can also result from inadequacy in addressing implications of emerging trends, including a lack of support for addressing new technologies (e.g., failure to support the necessary infrastructure for new technologies), and the failure to adequately address security concerns inherent in emerging technologies.

Finally, where governmental institutions are relatively weak, opportunity arises for individuals, groups, and agencies within government to gain from corruption. In essence, relatively weak governance can result in the inability of the government to control the actions of its agents, resulting in the creation of a risky business environment, which increases transaction costs for trade with the country. While bribery may immediately come to mind when we consider doing business in transition economies, from our perspective with regard to SCRM, those levels of corruption (Vargas-Hernandez 2011) that may favor certain parties to the exclusion of others should also be considered. One such area of concern is the relative prominence of corrupt activities in transition economies that subvert the mechanisms of the state to benefit those in power, which is frequently referred to as state capture (Hellman and Kaufmann 2001).

The challenge of state capture is that it disrupts the interactions between firms and the state and allows favored enterprises to gain unfair, anticompetitive advantages. As Hellman and Kaufmann (2001) note, a particularly devastating aspect is that the firms gaining such favor also manipulate governmental systems to prevent actions to reform the competitive environment. This leads to a circumstance in which state capture is both symptomatic of government failure and the cause of such failure. While the direct costs of corrupt practices can be substantial, indirect costs should also be considered.

In addition to the direct commission or omission of actions that impact global trade, we are also seeing a time when reactions to government policies and actions can disrupt supply chains. We have seen a large number of situations in which stakeholder's reactions to what is perceived as a lack of business responsiveness to a government's failure to act as a responsible party have resulted in risk to an organization's operations. One particularly remarkable recent example of public outcry driving reactions by business leaders is when the US President was viewed as not having reacted appropriately to a racially charged event in which a young woman was killed when a car operated by a member of a white supremacy group was driven into a group of protesters seeking the removal of monuments to controversial individuals supportive of the Confederate role in the US Civil War. Public outcry was directed at the perceived failure of the President to denounce the racial overtones of the confrontation, and business leaders were influenced toward stepping down from appointed roles in advisory councils established by the administration. In the end, a number of corporate chief executive officers from large businesses in the USA did resign from these appointments and the councils were disbanded (Gelles et al. 2017). While this occurred within a domestic environment, threats to organizational reputation and effectiveness can be substantially broadened when you are dependent on global supply chains (e.g., see Wright et al. 2007).

4 Supply Chain Risk from Outside the Central Government

When we consider reputational risk, new technologies can serve to create new avenues for risk. Effective SCRM in the modern era must recognize that it is easy for individuals to create a record of events, to broadcast those records, along with commentary, to vast numbers of people, and for groups to quickly mobilize to disrupt the business operations. This state of affairs requires constant vigilance regarding how events might be portrayed to the public in ways that damage a business or its supply partners in respect to stakeholder perceptions (Rice and Zegart 2018; Wright et al. 2007). Mobile phone recording and social media make every misstep a possible business disaster (just ask United Airlines about reactions to a recording of the removal of a passenger from a flight that went viral). The complexities of modern supply networks provide a great deal of potential for such damaging exposure. As Rice and Zegart (2018) point out, political risk extends well beyond the purview of traditional governmental actors in today's technology-enabled political environment.

SCRM practitioners must recognize that events beyond direct supplier performance involving members of our supply chains can impact our operations. Stakeholders have grown more sophisticated in finding the leverage points to influence bad actors in industry, and the methods involved often seek to disrupt purchasing firms so that they exert influence over their suppliers. In this chain of events, stakeholders have worked to make sure that our suppliers impact our reputations, and reactions of key stakeholders impact our business fortunes in today's connected environment (Wright et al. 2007).

Further, the role of individuals and groups outside of the central government can directly influence the business environment. Terrorism is an obvious example of such potential when threats or actual violence impact the environment in which we do business. While these threats have a long history, the growing impact can be seen in the numerous events with mass casualties that almost seem at times to dominate the news. Additionally, the breadth of the locations involved makes it quite clear that terrorism must be considered as a risk factor in our supply chains wherever we are doing business.

Finally, the extent to which modern supply chains are dependent upon the application of technology in a networked environment creates a new source of risk that can be delivered from anywhere at any time. While some governments, notably North Korea and Russia, have been implicated in cyber attacks that have impacted businesses, such attacks are readily perpetrated by groups and individuals without such connections. Security in this regard is incredibly important, and firms need to make sure that they are following the best possible current practice to ensure cyber security.

5 Managing the Risk

The first step for a firm is to consider how they want to deal with the new supply chain risk environment. While SCRM presents a broad array of challenges, it must also operate within the context of firm-wide policies. If your firm does not already have a clearly defined policy and set of procedures regarding international operations, now may be the time to encourage such a consideration. Broad understanding of the increasingly daunting environment within which our global supply chains operate may represent a point of leverage for supply management professionals in promoting serious consideration by organizational leadership of how they wish to address diplomacy in the face of the challenges presented above. In today's environment, one in which it appears that a quick and decisive response by an organization's domestic government is not guaranteed in response to damage to business interests, it is critical that organizations are clear about how they plan to engage with foreign governments (see, Chipman 2016). In many cases, this plan should be directed toward addressing what the firm intends to pursue in terms of displaying corporate social responsibility (CSR) in the global context.

Within SCRM, the range of alternatives to mitigate supply chain risk ranges from influence on political actors, to continued advocacy for trade agreements, and to strategies for leveraging alliances with domestic firms. The clear implication is that the only path forward is through business influence, and as previously noted, in many cases, this influence will need to overcome a race to the bottom as governments compete to settle the score by implementing a vicious cycle of coercive measures against one another. In a very broad sense, while some individual attention may resolve some areas of supply chain risk in the geopolitical realm, the far more typical case is that this truly is a sphere within which the mitigation of the risk is too big for the individual firm, and as such, effective strategies will generally require cooperative networks to approach solving these difficult supply chain risk challenges (Smith 2012).

In addition to work including groups of businesses in risk mitigation strategies, effective measures will also involve long-term engagement. Further, there will not be an effective substitute for a proactive stance. Firms need to work together to shape the environment that they experience. In this realm, a history of engagement with appreciative understanding of local conditions and sensitivities is critical. Developing a legacy of attention to the interests of all the key stakeholders, both in government and in the society, is central to managing geopolitical risk exposure. Public policies are generally collective in nature, so it makes sense that effective responses will generally require long-term collective action.

Engagement is a way to gain the opportunity to influence outcomes within society. From a bottom-up perspective, businesses can influence the social climate through advocacy and education that addresses the needs and concerns of key stakeholders, including the public at large. From the top-down perspective, such influence is aimed at political leaders themselves. Common approaches in this regard include the utilization of political action committees and lobbying. In the long term, the combination of these perspectives in an evolutionary approach, with changing methods as engagement progresses, is the form that best speaks to a truly proactive risk management stance. Such a stance also gains impact when a firm pursues collaboration with other businesses, industrial associations, and various stakeholder groups over a sustained presence in each region within which they operate or have supply chain impact. Even if a firm is not directly operating within a given jurisdiction, if members of their supply network are, the firm needs to consider the right level of engagement. In the modern environment, the fact that a firm is not directly operating within a particular region does not spare that firm from being held responsible for the actions of their suppliers. In the modern global supply chain, SCRM must be extended to all levels of the complex supply networks that support the success, or potentially spell the demise, of our organizations. The challenge is daunting, but fully embracing the task of SCRM in the tumultuous geopolitical climate is the only path toward success in the global economy.

References

Chipman, J. (2016). Why your company needs a foreign policy. *Harvard Business Review, 94*(9), 36–43.

Gelles, D., Landon, T., Ross Sorkin, A., & Kelly, K. (2017). Rebellion by business leaders spelled end of trump councils. *The New York Times*, A1.

Ghemawat, P. (2017). Globalization in the age of Trump. *Harvard Business Review, 95*(4), 113–123.

Global Agenda Council on Geo-economics (2016). *The age of economic coercion: How geo-politics is disrupting supply chains, financial systems, energy markets, trade and the internet*. World Economic Forum, White Paper, (http://ww3.eforum.rg/ocs/EF_ge_f_conomic_oercion.df).

Hellman, J., & Kaufmann, D. (2001). Confronting the challenge of state capture in transition economies. *Finance & Development, 38*(3), 31–35.

Keim, G. (2001). Business and public policy: Competing in the political marketplace. In M. Hitt, R. Freeman, & J. Harrison (Eds.), *Handbook of strategic management* (pp. 583–601). Malden, MA: Blackwell.

Khanna, P., & Mitachi, T. (2016). Supply chains as a coercive landscape. In: Global Agenda Council on Geo-economics (Eds.), *The age of economic coercion: How geo-politics is disrupting supply chains, financial systems, energy markets, trade and the internet.* World Economic Forum, White Paper, (http://ww3.eforum.rg/ocs/EF_ge_f_conomic_oercion.df).

Rice, C., & Zegart, A. (2018). Managing 21st-century political risk. *Harvard Business Review, 96*(3), 130–138.

Smith, M. E. (2012). Too big for the individual firm: Creating cooperative networks to solve difficult supply chain risk challenges. In O. Kahn & G. A. Zsidisin (Eds.), *Handbook for supply chain risk management: case studies, effective practices and emerging trends* (pp. 45–52). J Fort Lauderdale, FL: Ross Publishing.

Smith, M. E. (2016). Supply chain risk management in an era of economic coercion. In *16th International Research Seminar of Supply Chain Risk Management, International Supply Chain Risk Management Network.* Steyr Austria.

Toksöz, M. (2014). *Guide to country risk: How to identify, manage and mitigate the risks of doing business across borders*. New York: Perseus Book Group.

Vargas-Hernandez, J. (2011). The multiple faces of corruption: Typology, forms and levels. *Contemporary Legal and Economic Issues, 3,* 269–290.

Wright, C. M., Smith, M. E., & Wright, B. G. (2007). Hidden costs associated with stakeholders in supply management. *Academy of Management Perspectives, 21*(3), 64–82.

Index

G. A. Zsidisin and M. Henke (eds.), *Revisiting Supply Chain Risk*, Springer Series in Supply Chain Management 7, https://doi.org/10.1007/978-3-030-03813-7