

Supply Chain Risk Management: An Enterprise View and a Survey of Methods



Mikaella Polyviou, George Ramos, and Eugene Schneller

Abstract As supply chains have become more global and complex, supply chain disruptions have become more frequent (Resilinc. Supply chain disruptions-Resioinc's mid-year report. <https://www.resilinc.com/in-the-news/supply-chain-disruptions-resilincs-mid-year-report/>, 2021) and severe (Craighead et al. Decision Sciences 38(1):131–156, 2007). It is thus imperative for public and private enterprises to develop and implement strategies to prevent supply chain disruptions from occurring and recover quickly from them when they occur. Enterprises can do so by first establishing an effective supply chain risk management (SCRM) process that identifies, assesses, and proposes strategies to manage and monitor supply chain risks. In this chapter, we review the SCRM process and describe its four stages: risk identification, risk assessment, risk management, and risk monitoring. In doing so, we propose practices and strategies that help enterprises identify, assess, manage (accept, avoid, transfer, or mitigate), and monitor supply chain risks. We also provide examples of how enterprises across industries have implemented SCRM and identify key technologies employed within this process. Finally, we review recent research on behavioral influences in the context of SCRM. The chapter, overall, emphasizes the impact of continued risk for supply chains due to the COVID-19 pandemic. This chapter serves as a resource to academics, students, and practitioners into the SCRM process, actionable strategies employed within each stage of this process, and behavioral factors influencing it.

M. Polyviou (✉) · E. Schneller
Department of Supply Chain Management, W. P. Carey School of Business, Arizona State
University, Tempe, AZ, USA
e-mail: Mikaella.Polyviou@asu.edu

G. Ramos
Resilinc, Milpitas, CA, USA

1 Introduction

As supply chains have become more global and complex, enterprises operating in these supply chains have become more vulnerable to supply chain risks (World Economic Forum, 2013). Such vulnerabilities became apparent, for example, as the world faced the COVID-19 pandemic in 2019 through 2022. The pandemic has exposed the dependency of nations, hospitals, and businesses worldwide on Chinese suppliers and manufacturers for masks, gowns, and other protective equipment (Bradsher, 2020). It also exposed the bottlenecks and rigidity in supply chains after consumer demand for staples, such as toilet paper, yogurt, or meat, surged while industrial demand plummeted (Smith, 2020). As a result, the importance and consequences of not managing supply chain risks became clear to nations, public and private enterprises, and consumers.

Supply chain risks refer to “events or conditions that [have the potential to] adversely influence any part of a supply chain leading to operational, tactical, or strategic level failures or irregularities” (Ho et al., 2015, p. 5). They are characterized by the probability of their occurrence and the severity of their impact (Ho et al., 2015; Sheffi & Rice, 2005). Most supply chain risks are not “black swan” events (Taleb, 2007) but are common and predictable; thus, they may be considered “white swans” (Akkermans & Van Wassenhove, 2013, 2018). Supply chain risks that materialize often lead to supply chain disruptions, which refer to interruptions in the materials, services, information, or financial flow from one organization to another in a supply chain (Kim et al., 2015; Polyviou et al., 2018). Indeed, supply chain disruptions occur increasingly (Resilinc., 2021), with severe consequences for enterprises (Hendricks & Singhal, 2003, 2005).

Risks can disrupt not only an enterprise’s direct operations but also those of its trading partners, thereby disrupting the enterprise itself as a consequence. Indeed, the Business Continuity Institute revealed that the majority of supply chain disruptions experienced by an enterprise originated outside its boundaries: 48.9% of disruptions occurred at a first-tier supplier, 24.9% at a second-tier supplier, and 12.2% at a tier beyond second-tier suppliers (Business Continuity Institute, 2018).

Meanwhile, an enterprise might also be affected by disruptions occurring downstream in its supply chain. For example, a significant customer going out of business or changing course in product or service offerings can severely disrupt a supplier’s operations. In another example, farmers in the USA were forced to dump or dispose of milk and other fresh foods due to a significant drop in demand from restaurants, hotels, schools, and other food service providers at the beginning of the COVID-19 pandemic in the USA (Yaffe-Bellany & Corkery, 2020). As such, an enterprise does not operate in a vacuum. Instead, it depends on a network of suppliers, transportation and logistics providers, dealers, and others to receive and provide goods and services (Sheffi, 2005). Therefore, it needs to look outside its boundaries and work with its trading partners (suppliers, transportation providers, third-party logistics (3PL) providers, or customers) to identify and evaluate risks that can disrupt supply chain operations.

In this way, the academic literature advocates that enterprises focus on supply chain risk management (SCRM), namely the process of identifying, assessing, managing, and monitoring the risks that can disrupt their operations and supply chain networks (Ho et al., 2015). In this chapter, our objectives are to:

- Describe the SCRM process by outlining its stages
- Present the academic literature on each stage of the SCRM process and propose relevant methods and practices within each stage
- Discuss significant business examples that demonstrate effective SCRM
- Present recent academic literature on the behavioral influences in the context of managing supply chain risks and disruptions
- Present recent developments in SCRM in terms of technologies and software

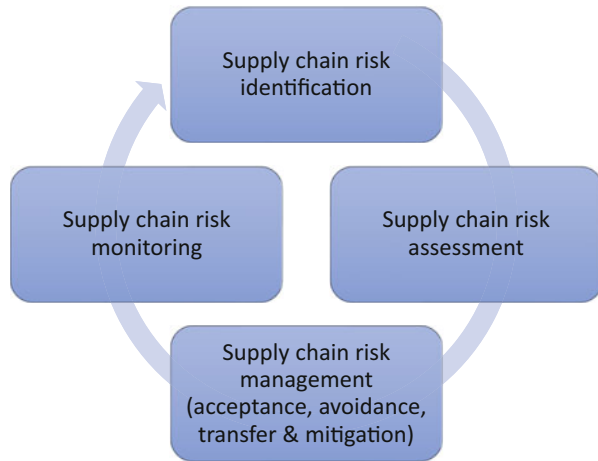
This chapter contributes to the literature in several ways. First, it provides a comprehensive review of methods employed to identify, assess, and mitigate supply chain risks. It also reviews the capabilities and supply chain strategies that enterprises can develop and implement to mitigate the probability and severity of supply chain disruptions proactively. Second, it makes a strong argument for an enterprise and network view of supply chain risks. The chapter emphasizes that an enterprise needs to look not only across functional silos and work with internal stakeholders (e.g., procurement, logistics, operations, sales, finance) but also beyond its boundaries and work with its trading partners (e.g., suppliers, customers, third-party logistics providers or government) to identify and evaluate risks that can disrupt supply chain operations. Finally, this chapter serves as a background resource to academics, students, and practitioners in the SCRM process, familiarizing all with actionable strategies employed within each stage and enhancing understanding of behavioral factors that can potentially influence this process.

2 Supply Chain Risk Management: An Overview

Supply chain risk management (SCRM) is defined as the process to identify, assess, manage, and monitor risks in the supply chain (Ho et al., 2015), as shown in Fig. 1. The stages in this process are summarized below:

1. **Supply chain risk identification:** This stage involves discovering all relevant risks that can influence an enterprise's operations and supply chain (Zsidisin & Henke, 2019). These risks might stem from internal and external sources relative to the boundaries of an enterprise (Christopher & Peck, 2004). Internal sources might be equipment breakdown, production delays, or accidents, while external sources may include natural disasters, pandemics, cyber-attacks, production or quality problems at suppliers' plants, or transportation accidents.
2. **Supply chain risk assessment:** Supply chain risks are typically characterized by the probability of their occurrence and the severity of their impact. This stage, as such, involves estimating these variables for the relevant supply chain risks

Fig. 1 The supply chain risk management (SCRM) process



identified in the risk-identification stage (Zsidisin & Henke, 2019). This stage also involves prioritizing the supply chain risks according to the enterprise’s risk tolerance.

3. **Supply chain risk management:** This stage involves identifying and developing strategies to reduce the probability or severity of the identified supply chain risks. This stage can include risk acceptance (i.e., doing nothing to mitigate the risk) and strategies to avoid, transfer, or mitigate risks (Chapman, 2006).
4. **Supply chain risk monitoring:** This stage involves evaluating the efficacy of the risk treatment strategies developed and implemented in the previous stage. It also includes identifying the opportunities to improve the stages of the SCRM process and updating the process based on the learnings gathered (Zsidisin & Henke, 2019).

We note that Fig. 1 depicts the SCRM process as a cycle, implying that the process is continuous. That is, the supply chain risk monitoring stage informs the supply chain risk identification, assessment, and management stages on an ongoing basis to ensure that the findings and decisions in each stage remain updated and relevant in a continuously changing business environment.

We also note that an enterprise must first be motivated to focus on SCRM and implement a program to identify, assess, mitigate, and actively monitor risks. This motivation is largely driven by the enterprise’s orientation toward supply chain risks and disruptions, formally defined as a “general awareness and consciousness of, concerns about, seriousness toward, and recognition of opportunity to learn from supply chain disruptions” (Bode et al., 2011, p. 837). An enterprise, which has a strong orientation toward supply chain disruptions, will consider them a critical issue and take actions that ensure continuity in its supply chain operations (Ambulkar et al., 2015; Bode et al., 2011).

Once an enterprise initiates an SCRM program, it will need to identify where the key vulnerabilities and failure points lie in its supply chain network and which customers need to be prioritized if a supply failure occurs. It also needs to evaluate its

Table 1 Supply chain risk management (SCRM) assessment questions*Assessment questions to ask internally about an enterprise's SCRM capabilities*

- What capacity is available, and how quickly can we redirect?
- Do we have emergency management structures and defined roles and responsibilities in place to respond to a crisis?
- How do we procure direct and indirect materials? How are supply chain disruptions accounted for in those procurement processes?
- Who is responsible for SCRM and crisis management at each site?
- What immediate action must we take to minimize loss and liability?
- Do you know your key support groups and their SCRM plans? Are your plans aligned so that you can continue operating?
- Do we need to prioritize customer demand? If so, which customers will be prioritized?
- What are the worst-case financial loss and legal exposure? Do you have a key contact list for individuals required to respond to a crisis?
- How long will it take to resume operations?

Assessment questions to ask suppliers about their SCRM capabilities

- What kinds of business functions are considered critical and have SCRM plans associated with them?
- What kinds of impacts are considered by your risk-mitigation and recovery-planning activities?
- How does senior management support the SCRM program? What management review and corporate governance mechanisms exist?
- Does your SCRM program ensure that all business processes and functions “critical” to your company are identified and documented?
- Does the SCRM documentation cover the components that make/support critical processes to an appropriate level of detail to ensure that single points of failure can be identified?
- Does your SCRM program ensure that business interruption risks are understood and prioritized and their impacts comprehended?
- Have your business groups taken steps to reduce risks?
- How frequently is the risk and impact assessment refreshed so that changes to your business are reflected in the SCRM program?
- Does your SCRM program ensure that the plans in place are well documented and current?
- Do these plans provide effective crisis response and ensure that critical operations continue during a crisis?
- Is the SCRM plan documentation readily available to the people who need it and maintain it?
- What kinds of exercises and drills are performed to ensure the completeness of the plans? Is the enterprise prepared to perform effectively during a crisis?
- Can your senior management confidently answer “Yes” when asked if everything reasonable and prudent has been done to be able to respond to and recover from an emergency?

Adapted from Zsidisin (2007)

current capabilities and those of its suppliers to manage supply chain risks. A CAPS Research study on business continuity management identified two sets of questions that an organization can ask internally and its suppliers when embarking on these initiatives (Zsidisin, 2007). We adjusted these questions to the SCRM context and provided them in Table 1.

3 Approaches to Identify, Assess, Manage, and Monitor Supply Chain Risks

3.1 Supply Chain Risk Identification

The first stage in the SCRM process is supply chain risk identification. This stage involves discovering all relevant risks that can disrupt an enterprise's operations. The objective of an enterprise in this stage should be to develop a risk register, namely a list of identified supply chain risks and a rating of their importance (Sodhi & Tang, 2012).

Risks that can interrupt the flow of materials, services, information, money, or even human resources in a supply chain are numerous. Examples include but are not limited to natural disasters (such as earthquakes, floods, or hurricanes), pandemics (such as the COVID-19 pandemic), geopolitical events (such as political unrest), labor strikes (such as strikes at plants or ports), accidents (such as transportation accidents), supplier-related disruptions (such as factory fires, product quality problems, or production bottlenecks), and security-related events (such as hacking and piracy). Other types of risks may not cause an interruption in the flow. Nevertheless, they may require adjustments to an enterprise's operations or influence its reputation, such as governmental policies and regulations (such as new environmental policies, tariffs, and other trade restrictions) or environmental incidents (such as oil spills). Table 2 presents a sample of the supply chain risk categories identified in the literature.

An enterprise can use different approaches to identify supply chain risks, as shown in Table 3. Every enterprise is responsible for identifying its own risks and typically does so from its own viewpoint (Hallikas et al., 2004). Nonetheless, it must work with key trading partners, such as suppliers, distributors, transportation providers, and customers, to identify and evaluate its dependencies on them and find where vulnerabilities might exist in the supply chain network beyond first-tier supply chain partners (Hallikas et al., 2004). For example, after a severe sub-supplier accident, Ericsson implemented a proactive SCRM approach. It began working with and required its first-tier suppliers to analyze, assess, and manage risks in their supply chains (Norrman & Jansson, 2004). Likewise, General Motors (GM) started working with its first-tier suppliers to assess if any second-tier suppliers were in trouble and proactively mitigate possible disruptions from those sub-tier suppliers (Banker, 2016).

Moreover, some types of enterprises, such as state or federal governments, have a responsibility to fulfill the needs of their constituents even after a supply failure or discontinuity. As such, they have to incorporate the needs and viewpoints of their stakeholders into their SCRM plans. For example, the US Federal Government maintains strategic national stockpiles of medicines and medical devices for use during public health emergencies, such as the COVID-19 pandemic (US Department of Health and Human Services, 2020).

Table 2 Categories of supply chain risks

Author	Concept	Risk categories
Harland et al. (2003)	Supply network risk	<ol style="list-style-type: none"> 1. Strategic risk 2. Operations risk 3. Supply risk 4. Customer risk 5. Asset impairment risk 6. Competitive risk 7. Reputation risk 8. Financial risk 9. Fiscal risk 10. Regulatory risk 11. Legal risk
Christopher and Peck (2004)	Supply chain risk	<ol style="list-style-type: none"> 1. Internal to the firm (Process; Control) 2. External to the firm but internal to the supply chain network (Demand; Supply) 3. External to the network (Environmental)
Manuj and Mentzer (2008)	Supply chain risk	<ol style="list-style-type: none"> 1. Supply risks 2. Demand risks 3. Operational risks 4. Security risks 5. Macro risks 6. Policy risks 7. Competitive risks 8. Resource risks
Tang and Tomlin (2008)	Supply chain risk	<ol style="list-style-type: none"> 1. Supply risks (Supply cost risk; Supply commitment risks) 2. Process risks 3. Demand risks 4. Intellectual property risks 5. Behavioral risks 6. Political/social risks
Wagner and Bode (2008)	Supply chain risk source	<ol style="list-style-type: none"> 1. Demand-side 2. Supply-side 3. Regulatory, legal, and bureaucratic 4. Infrastructure 5. Catastrophic
Rao and Goldsby (2009)	Supply chain risk	<ol style="list-style-type: none"> 1. Environmental risk sources 2. Industry risk sources 3. Organizational risk sources 4. Problem-specific risk sources 5. Decision-maker risk sources
Tummala and Schoenherr (2011)	Supply chain risk	<ol style="list-style-type: none"> 1. Demand risks 2. Delay risks 3. Disruption risks 4. Inventory risks 5. Manufacturing (process) breakdown risks 6. Physical plant (capacity) risks 7. Supply (procurement) risks 8. System risks 9. Sovereign risks 10. Transportation risks

(continued)

Table 2 (continued)

Author	Concept	Risk categories
Pettit et al. (2013)	Supply chain vulnerabilities	1. Turbulence 2. Deliberate threats 3. External pressures 4. Resource limits 5. Sensitivity 6. Connectivity
Ho et al. (2015)	Supply chain risk	1. Macro risks (Natural; Man-made) 2. Micro risks (Demand; Manufacturing; Supply; Infrastructural)

Adapted from Polyviou (2016)

3.2 Supply Chain Risk Assessment

The second stage in the SCRM process is supply chain risk assessment. This stage involves evaluating the probability of occurrence and the severity of impact of the supply chain risks identified in the first stage of supply chain risk identification. A key objective in this stage is for an enterprise to prioritize supply chain risks according to these variables so that it can focus on the high-priority risks. Table 4 provides exemplary methods that can be used to assess supply chain risks. Finally, an enterprise may use different metrics to measure severity, as shown below (Macdonald & Corsi, 2013; Simchi-Levi et al., 2014; US Department of Defense Standard Practice, 2012):

- The number of products affected
- The number of plant locations affected
- The number of customers affected by flow discontinuity
- The extent of damage to or loss of equipment or property
- The extent of damage to the environment
- The financial loss of the enterprise
- The time-to-recover (TTR): The time (e.g., in days or weeks) that a particular node in a supply chain network (e.g., a supplier's factory, a warehouse or distribution center, a transportation center) would need to become fully functional after a supply chain disruption has occurred (Simchi-Levi et al., 2015)

3.2.1 Supply Chain Risk Mapping and Prioritization

An enterprise is unlikely to have all the resources (time, physical, financial, human) to manage every possible risk that could affect its supply chain operations. Therefore, it needs to decide which risks to accept for the short- or long-term, manage actively, monitor actively but not manage, and require its suppliers to monitor. Notably, the enterprise needs to pay attention to the significant, apparent risks akin

Table 3 Methods to identify supply chain risks

Method	Description
Brainstorming	Method in which a team of experts collects a broad set of ideas and ranks them
Checklists	Method in which users refer to a previously developed list of representative supply chain risks that need to be considered
Check-sheets	Method in which users collect past data about events to derive an event's distribution. For example, an enterprise might record late deliveries from suppliers to rate supplier reliability
Delphi method	Multi-round process in which a group of experts anonymously replies to questionnaires about supply chain risks. At the end of each round, the experts receive feedback on the group's responses. The process repeats itself until expert consensus is achieved
Early warning signals	Indicators used to notify users of changing supply chain risks. For example, an enterprise may collect equipment maintenance information, machine reliability information, or product complaints as early indicators to predict supply chain risks
Fault tree analysis	Deductive method that begins with an undesired event (top event) and determines how that event could occur by constructing a logic diagram (i.e., the fault tree)
Failure mode and effects analysis (FMEA)	Method that identifies: (a) the ways in which a product or process can fail (i.e., failure modes) and (b) the consequences of those failures (i.e., effects). Failures can be prioritized according to their frequency, severity, and detectability
Hazard and operability study (HAZOP)	Inductive method that defines possible deviations from the expected or intended performance. "Guide words" are used as a systematic list to identify those deviations. Finally, the criticalities of the deviations are assessed
Interviews and surveys	Use of structured or semi-structured interviews and questionnaires to ask experts to identify supply chain risks
Ishikawa cause and effects diagram (Fishbone diagram)	Method that identifies possible causes for a problem. Causes are typically grouped into the following categories: Methods, Machines, People, Materials, Measurement, and Environment. This method can be used to facilitate brainstorming
Supply chain mapping	Method that involves the mapping of the supply chain network to identify the number and location of suppliers, number and origin of shipments, modes of transport and routes, ports, or 3PL providers. The supply chain map is then used to identify supply chain risks across the different nodes or arcs of the network
Wheel of crises	Method in which possible crises are listed in a wheel. Users turn the wheel and discuss the possible consequences if they face that crisis where the wheel stops. This method can be used to facilitate brainstorming

Based on Harland et al. (2003), Mitroff and Alpaslan (2003), Norrman and Jansson (2004), Peck (2005), Knemeyer et al. (2009), and Tummala and Schoenherr (2011)

Note: Other supply chain risk identification methods can be found in the British Standards Institution (BS 31100:2008) and ISO/ICE (ICE 31010:2019)

Table 4 Methods to assess supply chain risks

Method	Description
Bayesian analysis	Statistical technique that uses distribution data to assess the probability of occurrence of a supply chain risk
Bow-tie analysis	Method that describes and communicates risk scenarios. The bow-tie diagram gives a visual representation of all possible incident scenarios existing around a specific hazard. The bow-tie also shows what an enterprise does to control those scenarios by identifying safety barriers
Probability/severity matrix	Matrix that combines qualitative or semi-quantitative ratings of probability and severity of supply chain risks (see Fig. 2 for an example)
Event tree analysis	Inductive method that begins with a starting event (e.g., component failure) and determines the consequences of that event by constructing a logic diagram (i.e., the event tree). Each path is assigned a probability of occurrence. The user can then calculate the probability of the various possible outcomes
Expert opinion combined with historical data	Method that combines historical data about the occurrence of events (if available) with expert opinion on the events' probability of occurrence and severity of impact
Failure mode and effects analysis (FMEA)	Method that identifies: (a) the ways in which a product or process can fail (i.e., failure modes) and (b) the consequences of those failures (i.e., effects). Failures can be prioritized according to their frequency, severity, and detectability
Hazard and operability study (HAZOP)	Inductive method that defines possible deviations from the expected or intended performance. "Guide words" are used as a systematic list to identify those deviations. Finally, the criticalities of the deviations are assessed
Ishikawa cause and effects diagrams (Fishbone diagram)	Method that identifies possible causes for a problem. Causes are typically grouped into the following categories: Methods, Machines, People, Materials, Measurement, and Environment. This method can be used to facilitate brainstorming
Monte Carlo Simulation	Method used to establish the aggregate variation in a system that results from variations in the system for various inputs. Each input has a defined distribution, and the inputs are related to the output via defined relationships

Based on Harland et al. (2003), Mitroff and Alpaslan (2003), Normman and Jansson (2004), Zsidisin et al. (2004), Knemeyer et al. (2009), and Tummala and Schoenherr (2011)

Other supply chain risk assessment methods can be found in the British Standards Institution (BS 31100:2008) and ISO (ISO 31010:2019)

Some methods are relevant for supply chain risk identification and risk assessment and thus appear in Tables 3 and 4 of this chapter

to the "elephant in the room" that decision-makers tend to overlook. These risks are labeled as "gray rhinos" and are the high-probability and high-impact events that are generally ignored (Wucker, 2016). Gray rhinos do not occur suddenly but after a

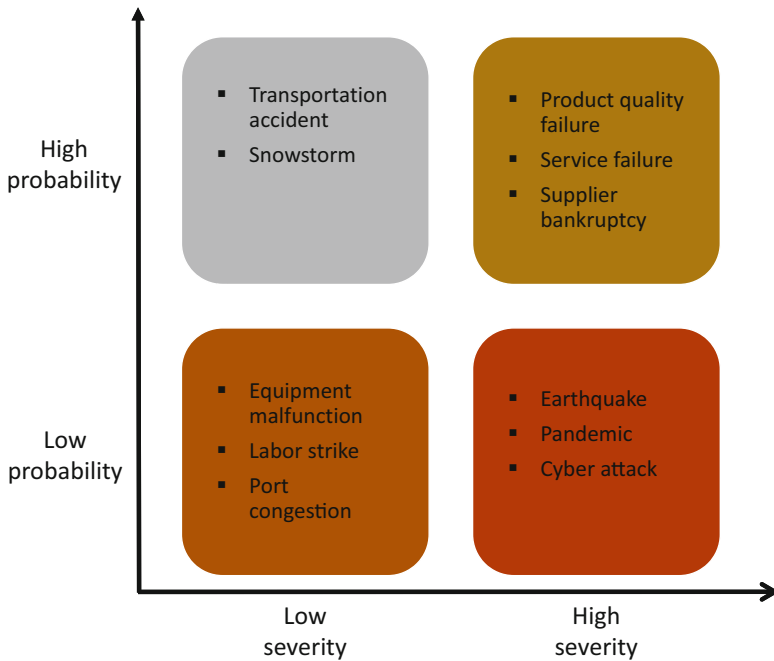


Fig. 2 Risk probability and severity matrix with supply chain risk examples

series of warnings and visible evidence, which decision-makers and organizations tend to overlook until too late (Wucker, 2016).

One method to guide decision-making around prioritizing the management of supply chain risks is to develop a matrix that categorizes them according to low versus high probability and low versus high severity. Figure 2 illustrates an example of such a matrix. Notably, an enterprise needs to define a time interval (e.g., a quarter or a year) by which it will update this categorization. The environment in which it operates changes continuously, and some risks might shift across categories. For instance, we indicated “port congestion” as a low-probability and low-severity event in the example depicted in Fig. 2. Nevertheless, port congestion in the USA in 2021, for instance, is likely considered a high-probability and high-severity event by many enterprises that import goods. In the summer and fall of 2021, the ports of Los Angeles and Long Beach are struggling to handle the overwhelming number of containers arriving—a result of a surge in US consumer demand for imported durable goods post-COVID-19. In this way, containers have been sitting on containerships in the water instead of being processed through the ports, disrupting the supply chain operations of companies such as Nike and Costco (Paris & Smith, 2021).

An enterprise may decide to focus first on high-probability and high-severity risks, as these are very likely to occur and will severely impact operations and disrupt supply continuity when they do occur. It could also focus first on the high-probability and low-severity risks. Even if these risks are not as severe, their frequent

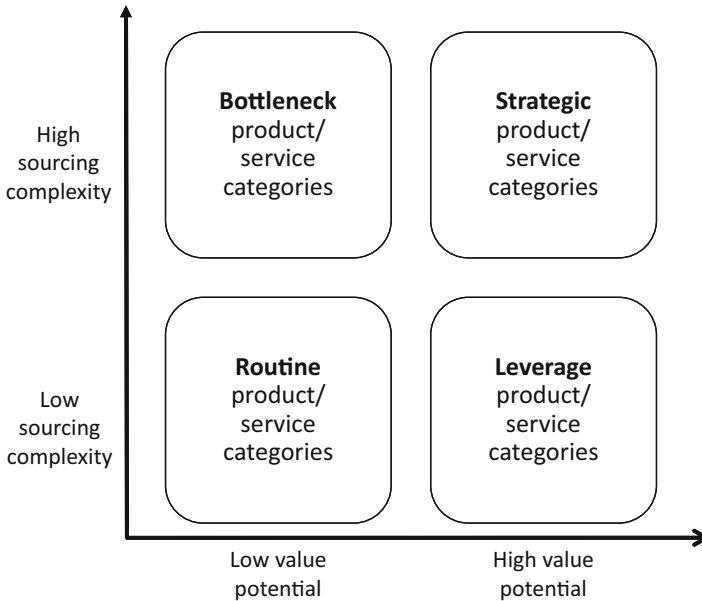


Fig. 3 Portfolio analysis matrix (Kraljic, 1983)

occurrence can accumulate costs and failures with severe long-term implications. Alternatively, it can focus on mapping the risks that exist within its boundaries (such as its plant locations or warehouses) or within its boundaries and at the first-tier suppliers and customers before considering risks in the sub-tiers of its supply chain.

An enterprise could also prioritize among first-tier suppliers and customers. A helpful way to do so is by using portfolio analysis to analyze its goods and services (Kraljic, 1983). With portfolio analysis, an enterprise can categorize goods and services according to their “value potential” (low versus high) and “sourcing complexity” (low versus high) (Kraljic, 1983).

Figure 3 shows a portfolio analysis matrix that can be constructed based on the product’s value potential and sourcing complexity. To assess “value potential,” metrics might include relative spend, impact to cost, delivery, and reliability, among others (Kraljic, 1983; Lambert, 2008). Metrics to assess “sourcing complexity” might include the number of available suppliers in the market, the complexity of materials requirements, product complexity, logistics complexity, and geographical locations of suppliers, among others (Kraljic, 1983; Lambert, 2008). Essentially, sourcing complexity represents the sourcing constraints that an enterprise will face when searching for alternative supply sources in case of a supply chain disruption. Commodity materials (e.g., those in the routine or leverage categories) typically pose a lower risk to an enterprise, as it can likely find alternative suppliers if a supply chain disruption occurs. Hence, the enterprise may not need to go beyond first-tier suppliers for its SCRM program. Conversely, materials that are sole-sourced or single-sourced (e.g., those possibly in the bottleneck or strategic categories) present



Fig. 4 Supply chain risk prioritization using a risk heat map

a significant risk of supply discontinuity. Therefore, the enterprise needs to closely monitor or work with those suppliers, search for risks beyond first-tier suppliers, and include those in its risk register. It is noteworthy that during COVID-19, items that many had categorized as commodities (e.g., masks and gowns), many of which were manufactured in China, turned out to be critical to the operation of health care organizations and the safety of both workers and patients. Therefore, one must be diagnostic as to the impact of any item as items are classified.

An enterprise can also include its risk tolerance or risk appetite, namely the amount of risk it is prepared to tolerate (be exposed to) at any time (Chapman, 2006), in the probability/severity matrix. Risk tolerance is unique to each enterprise and depends on its culture and objectives as well as the changing environmental conditions (Chapman, 2006).

Figure 4 shows an example of a risk heat map that combines the probability/severity matrix and risk tolerance. By considering its risk tolerance, an enterprise may first focus on the red areas before moving into the orange and yellow areas and decide to accept the supply chain risks in the green areas.

Once an enterprise identifies relevant supply chain risks, it can map them using different methods. For example, GM uses a concentric vulnerability map to map risks (see Fig. 5) (Sheffi, 2005). GM categorizes risks into strategic, financial, operations, and hazard risks. The axes correspond to low versus high probability of occurrence and low versus high impact. The radials show whether these risks originate from GM’s internal operations (e.g., at GM’s plants) or from the external environment (e.g., natural disasters).



Fig. 5 Concentric vulnerability map: A risk mapping tool (adapted from Sheffi, 2005)

3.2.2 Supplier Risk Assessments

A critical part of this stage in the SCRM process is supplier risk assessment. A supplier risk assessment constitutes a formal evaluation of the financial and operational risks that suppliers may exhibit. As enterprises typically do not have abundant resources to include all their suppliers in a formal supplier risk program, they use various criteria to decide on which ones to include. A recent survey of supply chain professionals by CAPS Research identifies the top criteria enterprises use, as shown in Table 5. Critical categories or spend areas are those categories that an organization considers essential to the business, either because they regard critical materials or materials that feed into multiple production lines. Annual spend represents the amount an enterprise spends with a supplier and is often an indicator of the supplier’s importance and, therefore, the amount of risk the supplier poses to the enterprise. Sole-sourcing is when an enterprise sources a particular good or service from one supplier, and only that supplier is available in the supply market (Van Weele, 2010). Single-sourcing is when an enterprise chooses to source a particular good or service

Table 5 Criteria used to include suppliers in a supplier risk program (CAPS Research, 2015)

Criteria used to determine if a supplier should be included in the supplier risk program	% of organizations surveyed
Critical categories/spend areas	82.8
Annual spend	70.3
Supplier product/ service is part of a critical deliverable	68.8
Sole- or single-source supplier	57.8
New supplier (never used before)	34.4
Certain geographic locations	29.7

from one supplier, even when other suppliers may be available in the market (Van Weele, 2010). Both these strategies can be risky as the enterprise depends on this one supplier, and anything the supplier does will influence the enterprise's supply chain operations. A new supplier in the supply base can also present risks because the enterprise has no experience working with this supplier and may be unfamiliar with its processes and general way of doing business. Finally, specific geographic locations may be considered riskier, for example, due to natural disaster risk, geopolitical tensions, trade restrictions, port congestion, or consistency in the quality of procured goods and services. Notably, the criteria in Table 5 could be considered indicators of "value potential" and "sourcing complexity," the two dimensions of Kraljic's portfolio analysis discussed above.

Supplier risk assessments are imperative given that most supply chain disruptions experienced by an enterprise originate in first-tier suppliers (Business Continuity Institute, 2018). Hence, enterprises can conduct formal supplier risk assessments, either internally or using a third party. The same CAPS Research survey mentioned above reported that 86% of the enterprises surveyed conducted supplier risk assessments, 79% scored those assessments, while 29% used third parties to conduct those assessments (CAPS Research, 2015).

3.3 Supply Chain Risk Management

The third stage in the SCRM process involves identifying, evaluating, and implementing strategies to manage the supply chain risks according to the enterprise's risk prioritization. Importantly, SCRM might not always involve mitigating risks, as an enterprise may accept, avoid, or transfer risks.

- **Supply chain risk acceptance:** An enterprise identifies and accepts the supply chain risk. It does not act either because it finds it economical not to do anything or has no alternative and feasible options to transfer or mitigate the risk (Chapman, 2006). Risk acceptance depends on the context in which an enterprise operates. For example, in the health care industry, hospitals can be captive to pharmaceutical manufacturers who hold a patent for a specific drug or medical device for a certain period of years. Hospitals, as such, often accept the risk of

sourcing these products. Risk acceptance also depends on the enterprise's risk tolerance or appetite (Chapman, 2006). As mentioned earlier in this chapter, risk tolerance is unique to each enterprise and depends on the enterprise's culture, objectives, industry sector, as well as environmental and business conditions (Chapman, 2006).

- **Supply chain risk avoidance:** An enterprise identifies the supply chain risk and considers it unacceptable. Because the enterprise cannot alter the risk, it chooses to eliminate it before the risk triggers a supply chain disruption (Ritchie & Brindley, 2007). Possible risk avoidance strategies include stopping the sale of a product, exiting a geographical market, or switching a supplier (Manuj & Mentzer, 2008).
- **Supply chain risk transfer:** An enterprise identifies the supply chain risk but transfers responsibility to another party. Possible risk transfer strategies include business interruption or supply chain disruption insurance (Cummings, 2020; Fan & Stevenson, 2018), outsourcing, financial risk transfer mechanisms, or risk-transfer contracts (Olson & Wu, 2010). Notably, risk transfer strategies may not eliminate an enterprise's exposure to the risk or the risk's impact. For instance, Hurricane Maria exposed the vulnerabilities of US hospitals, which relied on group purchasing organizations (GPOs) for a large amount of critical supplies with the notion that GPOs have a diversified supply base. In reality, GPOs were exposed to the same sub-tier suppliers.
- **Supply chain risk mitigation.** An enterprise identifies risk and actively manages it through actions that seek to reduce the probability of the risk's occurrence or the severity of its impact.

In this section, we focus on supply chain risk mitigation approaches. We refer the reader to Chapman (2006) for a more comprehensive review of the abovementioned approaches to supply chain risk avoidance and transfer. Indeed, the majority of the SCRM literature concentrates on supply chain risk mitigation. Table 6 offers an exemplary but not exhaustive list of such mitigation approaches.

We note that there are supply chain risks that an enterprise cannot anticipate. These risks can be highly improbable with highly severe consequences, typically regarded, as mentioned above, as "black swans" (Taleb, 2007), or they are inconceivable by management and organizational systems, typically regarded as "unknown-unknowns" (Ramasesh & Browning, 2014). The enterprise will be unable to develop specific risk mitigation strategies for these types of risks. Therefore, it must build resilience into its supply chain through (a) robustness strategies that help it avoid a supply chain disruption or resist its impact (such as anticipation and visibility capabilities) and (b) recovery strategies that help the enterprise recover from a supply chain disruption quickly (such as agile supply chain redesign) (Pettit et al., 2013; Wieland & Wallenburg, 2013).

Finally, even with a robust set of supply chain risk mitigation strategies available, an enterprise may be unable to implement certain strategies depending on various factors. In this chapter, we discuss two central factors influencing the ability of an enterprise to implement such strategies: the properties of the industry in which it operates and the attributes of its supply chain, specifically supply chain complexity.

Table 6 Exemplary supply chain strategies to mitigate the probability or impact of supply chain risks

Supply chain risk mitigation approach		References
Demand management approaches	Reduction of the forecast horizon	Sodhi and Tang (2012)
	Centralized (decentralized) capacity for unpredictable (predictable) demand, i.e., risk pooling	Chopra and Sodhi (2004, 2014)
	Shift demand across different products	Tang and Tomlin (2008)
	Flexible pricing	Tang and Tomlin (2008)
Supply management approaches	Flexible supplier contracts	Tang and Tomlin (2008)
	Risk-sharing contracts (buybacks, real option-based contracts)	Tang (2006)
	Multi-sourcing	Chopra and Sodhi (2004); Sheffi and Rice (2005); Pettit et al. (2013)
	Favor redundant supplies for high-volume products, low redundancy for low-volume products	Chopra and Sodhi (2004)
	Centralize redundancy for low-volume products to few, key, flexible suppliers	Chopra and Sodhi (2004)
	Supplier selection criteria	Ravindran et al. (2010)
	Supplier performance evaluation criteria	Blome and Schoenherr (2011)
Manufacturing management approaches	Modular product designs	Pettit et al. (2013)
	Multiple plants with interoperability	Sheffi and Rice (2005); Tang and Tomlin (2008)
	Manufacturing postponement	Pettit et al. (2013)
Transportation management approaches	Multiple transportation providers	Pettit et al. (2013)
	Multiple transportation modes	Pettit et al. (2013)
	Re-routing of requirements	Pettit et al. (2013)
Inventory management approaches	Logistics postponement	Zinn and Bowersox (1988)
	Strategic inventory	Pettit et al. (2013)
	Decentralized (centralized) inventory for predictable, lower-value products (for less predictable, higher-value products)	Chopra and Sodhi (2014)
Collaborative approaches with trading partners	Alliances with suppliers, group purchasing enterprises (GPOs), transportation providers, or distributors to identify, assess, share, or mitigate risks	Sheffi and Rice (2005); Pettit et al. (2013)
	Information sharing	Pettit et al. (2013)
	Collaborative Planning, Forecasting, and Replenishment (CPFR)	Pettit et al. (2013)
	Vendor-managed inventory (VMI)	
Product management approaches	Part commonality	Chopra and Sodhi (2004); Pettit et al. (2013)
	Product variability reduction	Pettit et al. (2013)

(continued)

Table 6 (continued)

Supply chain risk mitigation approach		References
	Favor responsiveness to cost for short life-cycle products, or low-volume, unpredictable products	Chopra and Sodhi (2004)
Capacity management approaches	Slack in capacity utilization	Sheffi and Rice (2005); Pettit et al. (2013)
	High redundancy for high-volume products and low redundancy for low-volume products	Chopra and Sodhi (2014)
	Distributed capacity	Pettit et al. (2013)
Financial management approaches	Hedging	Pettit et al. (2013)
	Portfolio diversification	Pettit et al. (2013)
Information management approaches	Information gathering about the business environment, competitors, suppliers, supply markets	Pettit et al. (2013)
	Monitoring and sharing information about early warning signals	Pettit et al. (2013)
General approaches	Business continuity plans internally and with suppliers	Zsidisin et al. (2005)

3.3.1 Industry Constraints and Supply Chain Risk Mitigation

The tolerance for risk and the implementation of supply chain risk mitigation strategies will depend on the industry in which an enterprise operates. For example, some industries, such as aerospace manufacturing or automotive manufacturing, were early adopters of just-in-time (JIT) manufacturing and delivery, leading to reduced inventories. Companies operating in these sectors recognized the need to employ other strategies to mitigate the risk of low buffers in the supply chain. Toyota, for example, seeks to standardize the parts it sources from Japanese suppliers so that the suppliers can share components that can be manufactured in several locations; asks suppliers of specialized parts, which cannot be duplicated across plants, to hold more inventory; and seeks to make parts procurement across geographic regions independent so that a natural disaster in Japan would not affect Toyota's production in other countries (Kim, 2011).

Furthermore, the degree of outsourcing differs across industries, which also influences an enterprise's dependency on its supply base. For example, industries, such as health care, have not only outsourced most of their procurement spend, but they frequently depend on sole or single suppliers, especially when the supplier holds the patent for the manufacturing of a drug or medical device. While this resource dependency (Pfeffer & Salancik, 1978) further increases supply chain risks, enterprises in this industry often accept the risk as a given.

3.3.2 Supply Network Complexity and Supply Chain Risk Mitigation

One stream of work explored how increasing complexity in the supply chain might increase the frequency and impact of supply chain risks. Broadly, supply chain complexity refers to “the level of detail complexity and dynamic complexity exhibited by the products, processes and relationships that make up a supply chain” (Bozarth et al., 2009, p. 80). Others viewed complexity as the combination of “the total number of nodes ... and the total number of forward..., backward..., and within-tier materials flows... within a given supply chain” (Craighead et al., 2007, p. 140).

Prior research largely demonstrated that supply chain complexity is detrimental when it comes to supply chain disruptions. For example, Choi and Krause (2006) argued that higher complexity in the supply base means an enterprise has to deal with many suppliers and, thus, monitor and coordinate more interfaces with those suppliers. Hence, Bode and Wagner (2015), argued that it becomes more difficult for the enterprise to continue having a sufficiently broad view and control over its suppliers, making it more susceptible to experiencing supply chain disruptions more frequently.

Furthermore, as complexity in the supply chain increases, the severity of supply chain disruptions can also increase. For example, Craighead et al. (2007) showed that if a trigger disrupts a part of the supply chain that is more complex, it is expected to affect more nodes or arcs in that network and, thus, increase the impact of the subsequent disruption. Also, Bode and Macdonald (2017) found that when complexity in a supply chain increases, managers are challenged to recognize that a supply chain disruption has happened as well as and diagnose it. This added difficulty can slow down an enterprise’s reaction to the supply chain disruption and subsequently exacerbate the disruption’s impact.

Recent research, however, has provided evidence that supply chain complexity may be both a detriment and a blessing for supply chains. Wiedmer et al. (2021) examined how various dimensions of supply network complexity (supply, logistics, and product) influence the ability of US automotive supply chains to resist and recover from supply chain disruptions triggered by the 2011 Japan Earthquake and Tsunami. Supply complexity (i.e., the number of suppliers) worsens disruption impact and improves a firm’s recovery from the disruption. Logistics complexity (i.e., the number of ocean carriers) does not significantly affect disruption impact but enhances a firm’s recovery. Lastly, product complexity (i.e., the number of components in a product) worsens disruption impact but does not significantly affect recovery. Wiedmer et al. (2021), as such, concluded that academics should differentiate between the various types of supply network complexity and the phase of the disruption in which an organization is (i.e., disruption-impact versus disruption-recovery phase).

3.4 *Supply Chain Risk Monitoring*

As enterprises change and evolve, so does supply chain risk. Hence, they need to regularly scan their internal operations, supply chain network, and external environment to identify new sources of risks or how the already identified risks may have changed. They also need to evaluate whether the established supply chain risk mitigation strategies are effective. This stage is formally labeled as supply chain risk monitoring. Activities in this stage include:

- Updating the risk register if necessary
- Appraising the effectiveness of the supply chain risk mitigation actions. Metrics that can be used to assess effectiveness include time to diagnose a supply chain disruption and implement recovery strategies, time to recover, time to set up alternative sources, operational metrics (such as on-time delivery, lead time), or the number of risk events affecting the supply chain. For specific types of supply chain disruptions, such as product recalls, other metrics can be used, such as the number of downstream partners notified about the recall, the number of responders to the recall notification, the percentage of recalled products, or the time to remove a product from the market
- Evaluating the effects of the risk treatment on the performance of the enterprise (such as product or service quality, on-time delivery, and lead time)
- Identifying opportunities for improvement
- Considering changes in regulations, processes, performance assessment, and the supply chain to update the SCRM plan
- Monitoring how supply chain partners are performing relative to their commitments

Academic research has paid little attention to supply chain risk monitoring (Fan & Stevenson, 2018; Ho et al., 2015). Researchers advised that firms develop data management information systems to monitor risks (Tummala & Schoenherr, 2011) and establish processes to identify and monitor early warning signals (Craighead et al., 2007) to identify new risks or observe trends proactively. Sheffi (2005) has identified the importance of studying “near misses,” namely incidents that, if actually occurred, or occurred more frequently or for more extended periods, would have a significant impact and provide the occasion to opine on ways one might act. This takes a significant commitment to vigilance and deterrence. However, there is an important temporal aspect to this—as no risk, as discussed later in this chapter, of the breadth and depth of COVID-19 has occurred in many years. Denial or a lack of incentives, including costs associated with long-term vigilance by management and executive boards, may interfere with a methodical, disciplined, and prudent approach to existing SCRM routines that focus on short-term and more manageable risks (e.g., hurricanes and factory fires). In practice, enterprises tend to incorporate supply chain risk monitoring into existing enterprise routines (Fan & Stevenson, 2018). When it comes to monitoring supplier financial or operational risk, enterprises tend to incorporate it into their regular supplier assessment activities

Table 7 Assessments of highest-risk suppliers (CAPS Research, 2015)

Regularity of supplier risk assessments	% of companies surveyed
Quarterly	30.2
Yearly	23.8
Six months	20.6
Monthly	6.3
Other	12.7

(Blome & Schoenherr, 2011). For instance, CAPS Research reported that most organizations re-assess the highest-risk suppliers quarterly, followed by yearly and bi-annually, as shown in Table 7.

3.4.1 Technologies for Supply Chain Risk Monitoring

Enterprises increasingly utilize specialized software to monitor the risks in their supply chain. Interviews we conducted with supply chain managers from various industries show that best-practice organizations typically employ third-party tools to monitor risks in their supply chains on a real-time basis. For example, Credit Risk Monitor and Dun & Bradstreet’s Supplier Risk Manager are popular tools to monitor supplier financial risk. Other tools, such as supply chain network mapping software by Resilinc or Risk Methods, enable enterprises to map their supply chain networks, monitor events that can affect critical nodes or arcs in the network in real-time, and promptly act on threats for supply continuity. Other examples of such software are shown in Fig. 6. These types of software often use technologies including artificial intelligence and machine learning, as shown in Fig. 6.

A recent development in supply chain management has been the use of control towers. In the supply chain context, control towers are cloud-based, digital networks that provide executives visibility into their trading partners and the supply chain. For example, intelligent control towers can help mitigate supply chain risks by providing visibility into events occurring in the supply chain network, identifying how such events can influence lead times based on the enterprise’s service-level agreements, offering suggestions for mitigating the risks using artificial intelligence, and even executing these suggestions without human intervention (One Network, 2020).

4 Behavioral Influences in Supply Chain Risk Management

Recent research has begun extending inquiry around SCRM beyond the traditional supply chain tactics to mitigate risks and exploring behavioral supply management issues. Carter et al. (2007, p. 634) define behavioral supply management as “the study of how judgment in supply management decision-making deviates from the assumptions of homo economicus.” Recent research examined behavioral issues

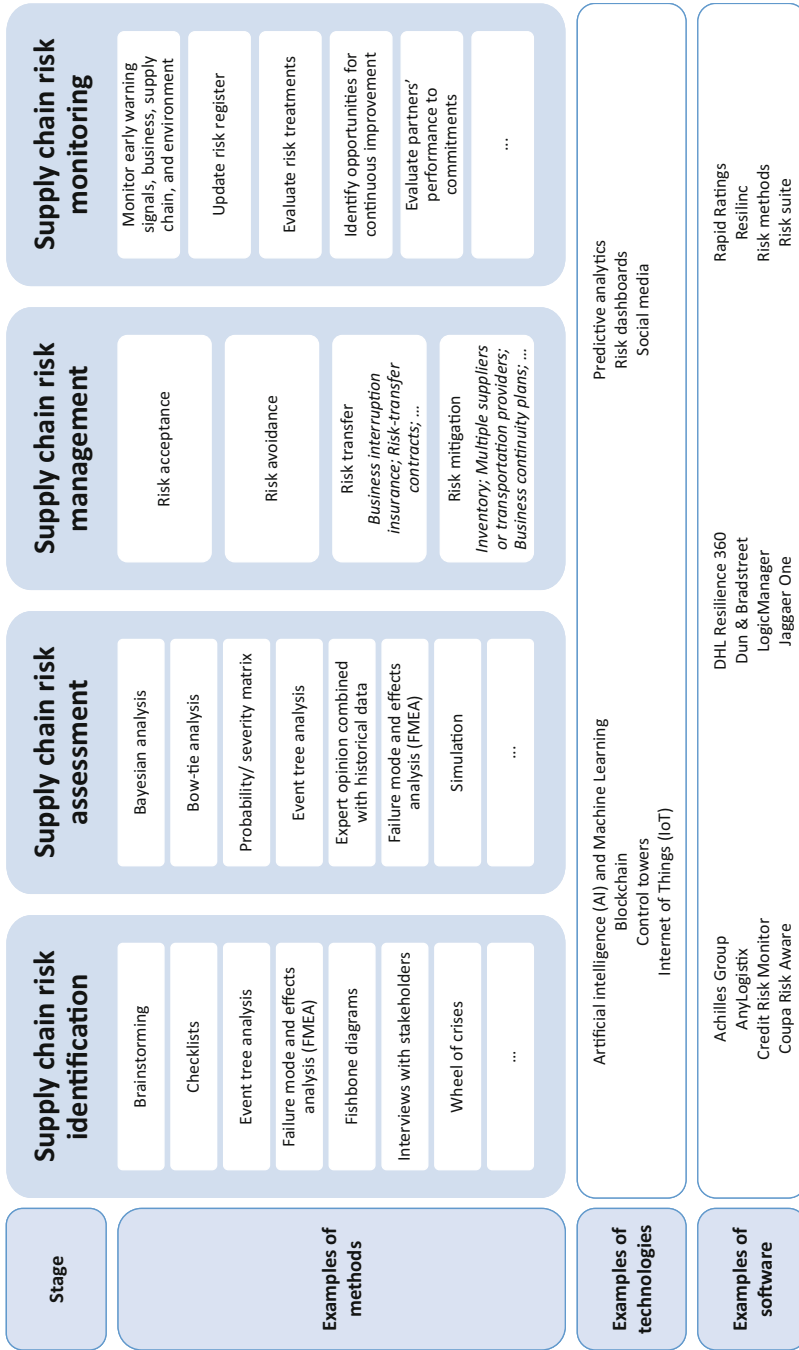


Fig. 6 The supply chain management (SCRM) process with examples of methods, technologies, and software

surrounding the identification, assessment, and mitigation of supply chain risks and reactions following a supply chain disruption. Ellis et al. (2010) were among the first to propose and demonstrate empirically that managerial risk perceptions matter when it comes to risk mitigation strategies. The authors showed that supply market characteristics (such as technological uncertainty and availability of suppliers) and product characteristics (such as the degree of importance and customization of a product) influence managerial perceptions of the probability and severity of supply chain disruptions, and in turn, their search for alternative suppliers.

Eckerd and colleagues focused on psychological contract breaches, which occur when “an individual perceives insufficient fulfillment of obligations from an exchange partner” (Eckerd et al., 2013, p. 568). A breach, as such, is a perception that the terms in a psychological contract have been violated or simply not met (Suazo, 2011). Eckerd et al. (2013) found that breach attribution and severity perceptions influence a buyer’s ordering behavior. These attributes also trigger an adverse affective reaction, termed psychological contract violation, which influences a buyer’s perception of how fair a supplier is. Similarly, Mir et al. (2017) found that breach attribution and severity elicit negative affective reactions, which, in turn, influence supplier switching. Lastly, Eckerd et al. (2016) extended this previous work to examine the role of national culture (China vs. the USA). They found that breach attribution influences post-breach ordering behavior and that breach severity and national culture influence trust towards the supplier.

Other studies explored how an enterprise’s communication about risk and resilience influences sourcing decisions. For example, DuHadway et al. (2018) showed that individuals make riskier sourcing decisions after their enterprises communicate progress in reducing supply chain risk levels. Likewise, Mena et al. (2020) found that managerial perceptions of enterprise resilience via systemic communication of resilience initiatives, such as training or corporate announcements by the company’s executives or via personal exposure motivate managers to select riskier suppliers. This effect was strengthened when the risk propensity of a decision-maker was higher.

Other researchers focused on the effects of supply chain disruptions on affective reactions and supply management decisions post disruption. For example, Reimann et al. (2017) looked at supplier-included disruptions and examined the conditions that induce buyers to engage in constructive interaction with their suppliers or create conflict between buyers and suppliers. Finally, two studies by Polyviou and colleagues examined the role of emotions in response to supply disruptions and post-disruption sourcing decisions. Polyviou et al. (2018) demonstrated that sourcing managers experience more anger when they consider a supply disruption as controllable by a disrupting supplier rather than nature; as a result, they are less likely to keep sourcing from that supplier afterward. Polyviou et al. (2022) found that sourcing managers experience more guilt following a supply disruption they consider controllable by a disrupting supplier rather than nature, and they had recommended that supplier to their organization before the disruption. In turn, they tend to prefer riskier yet more advantageous suppliers when making new supplier selections after the disruption. In other words, Polyviou et al. (2022)

showed there is a path dependency between prior and new supplier selection decisions when the previously selected supplier later becomes a disrupting supplier. Finally, Chen et al. (2019) found evidence for the “positive supplier performance penalty effect” (p. 1224) such that sourcing managers are more likely to terminate a supplier with stellar performance when that supplier commits an error.

In summary, this literature stream has demonstrated that responses to supply chain risks and disruptions are influenced by the characteristics of the individuals making the decisions, the firm experiencing the risk or disruption, and the environment. Therefore, researchers must not only focus on proposing traditional supply chain strategies to mitigate risks but also on further understanding the cognitions, emotions, and other non-objective factors that can influence decision-making in this context.

5 The Governance Structure of Supply Chain Risk Management: Where Does Risk Responsibility Lie?

Little academic research focuses on the governance structure around SCRM. Although SCRM is traditionally considered everyone’s job (Sheffi & Rice, 2005), an enterprise must establish a governance structure around it. The Supply Chain Risk Leadership Council (SCRLC) (2011) offers generic guidelines about a governance structure for risk management. According to SCRLC (2011), an enterprise developing an SCRM program should start with a cross-functional team of decision-makers, including quality, engineering, operations, supply management, logistics, finance, legal, or marketing managers. This team will identify, own, and manage risks at the level they exist, and determine the SCRM program’s scope. An enterprise, however, needs to go beyond these guidelines and establish a formal governance structure around SCRM. A governance structure has several benefits, as follows:

- Establishes a formal SCRM process
- Determines formal accountability and ownership of supply chain risks
- Sets the system within which cross-functional managers will come together to identify, evaluate, and alleviate supply chain risks
- Establishes formal channels of communication among the various stakeholders
- Determines the frequency of supply chain risk monitoring and continuous update of the risk register
- Establishes a performance measurement system to assess the efficacy of the SCRM practices implemented not only by the focal enterprise but also by its key trading partners
- Provides the incentives for continuous improvement in SCRM
- Encourages change in the behavior within and beyond the enterprise to truly make SCRM everyone’s job

6 Supply Chain Risk Management in the Post-COVID-19 Era

The COVID-19 pandemic brought to the forefront the importance of many of the issues discussed above across many industries. Indeed, it presented a continuing “live study” to understand supply chain disruptions and approaches to alleviate them (Chopra et al., 2021) and brought the importance of large-scale/long-term SCRM efforts to the forefront. The pandemic disrupted supply chains around the globe, impacting production and logistics operations and reducing opportunities to meet the surge in demand for consumer products. Less than 6 months into the pandemic, 94% of Fortune 1000 companies incurred supply chain disruptions triggered by COVID-19, while 75% were negatively affected (Timmermans et al., 2020). Vulnerabilities of supply chains to an external shock such as a pandemic—in concert with little attention by management to plans for regaining resilience—left supply chains across the globe in shambles (Timmermans et al., 2020).

In the USA, the newly elected President Biden issued executive orders focused on managing supply chain risks (The White House, 2021a, 2021b). The EU’s “Action Plan on Critical Raw Materials” (European Commission, 2020) presented cross-national strategies to develop a secure and sustainable supply of raw materials for a resilient European economy. The pandemic highlighted the importance of supply chains and SCRM as keys to sustainability and what many have described as a need to “future proof” the supply chain.

The COVID-19 pandemic led to reflection on the unanticipated effects of supply chain practices. For example, the health sector in the USA had embraced JIT inventory and an overemphasis on cost, and it relied on a number of intermediaries (GPOs and distributors) to carry out the sourcing and contracting on behalf of hospitals. However, hospitals across the globe were strained as they had continuously escalated their contracting with a few suppliers, many of whom were located far from their shores. Such single sourcing (see Table 5) and contracting were frequently done without adequate credentialing of suppliers and their suppliers’ upstream suppliers, with little network mapping software in place. Indeed, a domino effect could be observed as shortages cascaded. Few health care providers subscribed to the services that detect suppliers’ risks.

Disruptions to the health sector supply chain were not a new occurrence. In 2017, the aforementioned Hurricane Maria closed down important suppliers in Puerto Rico—many of which were the sole source for medical goods and operated in an environment that had little investment in pre-disaster mitigation, adaption, and planning as well as little building and maintaining of relationships with diverse partners, businesses and stakeholders—all of which hampered the recovery effort (Kim & Bui, 2019; Sacks et al., 2018). The result of poor disaster management was that healthcare organizations in the USA were forced to postpone elective surgeries and ration critical products (Sacks et al., 2018).

COVID-19 exposed many of the risks associated with global sourcing. In the health care and other sectors, many products were produced in Asia. As those

nations secured their domestically manufactured products for their populations, the surges in demand for products in other nations, such as the USA, were not met. Moreover, as shipping became difficult and tariffs were imposed, supply chain disruptions were exacerbated. With a rapidly accelerating demand, the hypergrowth in semiconductor chip demand has significantly impacted the availability of chip-powered equipment. While much focus has been on the auto industry, in the biotech sector, devices such as ventilators and defibrillators, imaging machines, monitors (for glucose and blood pressure), and implantable devices are all dependent on the availability of semiconductor chips, leading companies to consider strategies to mitigate both current and long-term risks (Murray & Bradley, 2021).

One of the conclusions to be drawn from the COVID-19 experience is the inadequacy of ongoing management strategies for dealing with significant periods of uncertainty. As discussed above, governance is an essential aspect of any SCRM program. Health care systems across the USA and other countries had relied on government-sponsored and managed pooled resources. And while pools can be an important part of an SCRM program, many of these stockpiles failed to provide significant quantities of needed products and, when provided, products had not been properly maintained or rotated as expiration dates occurred (Handfield et al., 2020). Common pool resources require a strong governance and management structure.

How should managers be thinking? COVID-19 presented an unusual situation with (a) a sizeable demand increase, (b) a significant dip in supply, and (c) great uncertainty as to the duration of the pandemic. It is an example of an extreme supply chain risk requiring new ways of addressing risk and thinking about new models for supply chain resilience (Sheffi, 2020). Stimulated by this tri-factor situation, researchers have begun to differentiate between strategies and governance systems required for “micro,” “meso,” and “macro” supply chain disruptions (Azadegan & Dooley, 2021) and strategies associated with different kinds of disruptions (Chopra et al., 2021). SCRM strategies include pools of supplies and capabilities owned by an individual company for use at a time of minimal disruption, tiered, within-industry collaboration of supplies for somewhat longer disruptions, and larger pools of well-managed common goods, generally sourced and managed by the government or their well-managed surrogate, to assure resilience. Noteworthy is the “macro” effort identified by Azadegan and Dooley (2021), which recognizes the role of government and association-sponsored pools, which largely failed in their ability to meet the supply chain disruptions associated with COVID-19 (Handfield et al., 2020) in developing common repositories and strategies.

Over the months of the COVID-19 pandemic, there has been much discussion about “future-proofing” the supply chain and putting forth a “new normal.” Needed is a thorough understanding of the markets in which an organization operates and the markets in which trading partners operate. Absent early in the pandemic, in the health care and other sectors, was adequate visibility into the market, understanding of extant and potential resources, and a governance system to manage existing resources (Butt, 2021; Finkenstadt & Handfield, 2021). Clearly, COVID-19 was a critical wake-up call as there has been a rapid evolution in developing and implementing technologies to achieve end-to-end visibility (Sharma et al., 2020).

This discussion of COVID-19 reveals the need for different SCRM strategies to prepare for and mitigate supply chain disruptions of different duration and impacts on an entire industry. The health sector, highlighted in our discussion, is just one of many sectors impacted. Lingering questions include the benefits and costs of reshoring, the likelihood of competitors working collaboratively, the role of government and public–private entities as a buffer, and the financing of resilience initiatives. The World Health Organization had long warned that there were substantial risks for a pandemic of the nature of COVID-19, the West Pacific Region was a hotspot for outbreaks, and there was a need to “establish mechanisms to ensure the timely supply and availability of PPE, vaccines, drugs and other materials to ensure the safety and well-being of healthcare workers, patients and visitors and the broader community at all levels of the healthcare system” (World Health Organization, 2017). With predictions that we may well face such threats, supply chain management and other disciplines must coordinate and collaborate in preparing for future pandemics (World Economic Forum, 2021). After all, predictions show that the next global pandemic, as severe as COVID-19, will occur with a 47–57% chance within the next 25 years (Smitham & Glassman, 2021). Supply chain risk identification, assessment, management, and monitoring are, indeed, necessary and ongoing sub-processes.

7 Conclusions

In this chapter, we provided an overview of the SCRM process. We presented methods to identify, assess, manage, and monitor supply chain risks. We also discussed factors, such as industry and supply chain complexity, which can constrain an enterprise in implementing specific supply chain risk mitigation approaches. Furthermore, we presented research that argues that SCRM is not merely a logical business process but can be influenced by behavioral and other non-objective factors. These factors may include attributes of the supply chain risk manager, the risk, or the disruption. Finally, we argued that SCRM should be everyone’s job. Nonetheless, this process must be formalized in organizations so that it receives the attention it deserves. Figure 6 summarizes the discussion in this chapter.

Importantly, organizations must realize that they will be unable to identify and assess all possible risks that can disrupt their supply chain operations. There will be those “unknown unknowns,” namely uncertainties of which management will be unaware and, thus, unprepared to manage (Ramasesh & Browning, 2014). As such, organizations need to go beyond SCRM and cultivate resilience in their supply chain systems. Building resilience goes beyond risk mitigation; it involves the identification of system capabilities that are not risk-specific but can address a variety of supply chain risks (Fiksel et al., 2015). Resilience, moreover, enables an organization to deal with supply chain risks and disruptions more effectively than its competition and thus gain a competitive advantage (Sheffi & Rice, 2005).

References

- Akkermans, H. A., & Van Wassenhove, L. N. (2013). Searching for the grey swans: The next 50 years of production research. *International Journal of Production Research*, *51*(23–24), 6746–6755.
- Akkermans, H. A., & Van Wassenhove, L. N. (2018). A dynamic model of managerial response to grey swan events in supply networks. *International Journal of Production Research*, *56*(1–2), 10–21.
- Ambulkar, S., Blackhurst, J. V., & Grawe, S. (2015). Firm's resilience to supply chain disruptions: Scale development and empirical examination. *Journal of Operations Management*, *33–34*(1), 111–122.
- Azadegan, A., & Dooley, K. (2021). A typology of supply network resilience strategies: Complex collaborations in a complex world. *Journal of Supply Chain Management*, *57*(1), 17–26.
- Banker, S. (2016, May 31). General Motors embraces supply chain resiliency. *Forbes*. <https://www.forbes.com/sites/stevebanker/2016/05/31/general-motors-embraces-supply-chain-resiliency/#ca0e9f83684>.
- Blome, C., & Schoenherr, T. (2011). Supply chain risk management in financial crises—A multiple case-study approach. *International Journal of Production Economics*, *134*(1), 43–57.
- Bode, C., & Macdonald, J. R. (2017). Stages of supply chain disruption response: Direct, constraining, and mediating factors for impact mitigation. *Decision Sciences*, *48*(5), 836–874.
- Bode, C., & Wagner, S. M. (2015). Structural drivers of upstream supply chain complexity and the frequency of supply chain disruptions. *Journal of Operations Management*, *36*(3), 215–228.
- 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.
- Bozarth, C. C., Warsing, D. P., Flynn, B. B., & Flynn, E. J. (2009). The impact of supply chain complexity on manufacturing plant performance. *Journal of Operations Management*, *27*(1), 78–93.
- Bradsher, K. (2020, July 5). China dominates medical supplies, in this outbreak and the next. *The New York Times*. <https://www.nytimes.com/2020/07/05/business/china-medical-supplies.html>.
- British Standards Institution (BS 31100). (2008). *Code of practice for risk management*. <https://shop.bsigroup.com/ProductDetail/?pid=00000000030153956>.
- Business Continuity Institute. (2018). *Supply chain resilience report*. <https://www.thebci.org/news/bci-supply-chain-resilience-report-2018.html>.
- Butt, A. S. (2021). Strategies to mitigate the impact of COVID-19 on supply chain disruptions: a multiple case analysis of buyers and distributors. *The International Journal of Logistics Management*. Ahead-of-print. <https://doi.org/10.1108/IJLM-11-2020-0455>
- CAPS Research. (2015). *Managing supplier risk*. <https://www.capsresearch.org/library>.
- Carter, C. R., Kaufmann, L., & Michel, A. (2007). Behavioral supply management: A taxonomy of judgment and decision-making biases. *International Journal of Physical Distribution and Logistics Management*, *37*(8), 631–669.
- Chapman, R. J. (2006). *Simple tools and techniques for enterprise risk management*. Wiley.
- Chen, Y. S., Rungtusanatham, M. J., & Goldstein, S. M. (2019). Historical supplier performance and strategic relationship dissolution: Unintentional but serious supplier error as a moderator. *Decision Sciences*, *50*(6), 1224–1258.
- 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.
- Chopra, S., & Sodhi, M. (2014). Reducing the risk of supply chain disruptions. *MIT Sloan Management Review*, *55*(3), 72–80.
- Chopra, S., Sodhi, M., & Lücker, F. (2021). Achieving supply chain efficiency and resilience by using multi-level commons. *Decision Sciences*, *52*(4), 817–832.

- Chopra, S., & Sodhi, M. S. (2004). Supply-chain breakdown. *MIT Sloan Management Review*, 46(1), 53–61.
- Christopher, M., & Peck, H. (2004). Building the resilient supply chain. *International Journal of Logistics Management*, 15(2), 1–13.
- 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.
- Cummings, S. (2020, November 1). A quick guide to insurance for supply-chain disruption. *Supply Chain Brain*. <https://www.supplychainbrain.com/blogs/1-think-tank/post/32135-a-quick-guide-to-insurance-for-supply-chain-disruption>.
- DuHadway, S., Carnovale, S., & Kannan, V. R. (2018). Organizational communication and individual behavior: Implications for supply chain risk management. *Journal of Supply Chain Management*, 54, 3–19.
- Eckerd, S., Boyer, K. K., Qi, Y., 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.
- Eckerd, S., Hill, J., Boyer, K. K., Donohue, K., & Ward, P. T. (2013). The relative impact of attribute, severity, and timing of psychological contract breach on behavioral and attitudinal outcomes. *Journal of Operations Management*, 31(7–8), 567–578.
- 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.
- European Commission. (2020). Critical raw materials resilience: Charting a path toward greater security and sustainability. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0474>.
- Fan, Y., & Stevenson, M. (2018). A review of supply chain risk management: definition, theory, and research agenda. *International Journal of Physical Distribution and Logistics Management*, 48(3), 205–230.
- Fiksel, J., Polyviou, M., Croxton, K. L., & Pettit, T. J. (2015). From risk to resilience: Learning to deal with disruption. *MIT Sloan Management Review*, 56(2), 79–86.
- Finkenstadt, D. J., & Handfield, R. (2021). Blurry vision: Supply chain visibility for personal protective equipment during COVID-19. *Journal of Purchasing and Supply Management*. <https://doi.org/10.1016/j.pursup.2021.100689>
- Hallikas, J., Karvonen, I., Urho, P., Virolainen, V.-M., & Tuominen, M. (2004). Risk management processes in supplier networks. *International Journal of Production Economics*, 90(1), 47–58.
- Handfield, R., Finkenstadt, D. J., Schneller, E. S., Godfrey, A. B., & Guinto, P. (2020). A commons for a supply chain in the post-COVID-19 era: The case for a reformed strategic national stockpile. *The Milbank Quarterly*, 98(4), 1058–1090.
- Harland, C., Brenchley, R., & Walker, H. (2003). Risk in supply networks. *Journal of Purchasing and Supply Management*, 9(2), 51–62.
- 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. (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.
- 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.
- ISO/ICE (ICE 31010:2019). Risk management—Risk assessment techniques. <https://www.iso.org/standard/51073.html>.
- Kim, C. R. (2011, September 6). Toyota aims for quake-proof supply chain. *Reuters*. <https://www.reuters.com/article/us-toyota/toyota-aims-for-quake-proof-supply-chain-idUSTRE7852RF20110906>.
- Kim, K., & Bui, L. (2019). Learning from Hurricane Maria: Island ports and supply chain resilience. *International Journal of Disaster Risk Reduction*, 39, 101244.

- Kim, Y., Chen, Y.-S. S., & Linderman, K. (2015). Supply network disruption and resilience: A network structural perspective. *Journal of Operations Management*, 33–34, 43–59.
- Knemeyer, A. M., Zinn, W., & Eroglu, C. (2009). Proactive planning for catastrophic events in supply chains. *Journal of Operations Management*, 27(2), 141–153.
- Kraljic, P. (1983). Purchasing must become supply management. *Harvard Business Review*, 61(5), 109–117.
- Lambert, D. M. (2008). *Supply chain management: processes, partnerships, performance* (3rd ed.). Supply Chain Management Institute.
- Macdonald, J. R., & Corsi, T. M. (2013). Supply chain disruption management: Severe events, recovery, and performance. *Journal of Business Logistics*, 34(4), 270–288.
- Manuj, I., & Mentzer, J. T. (2008). Global supply chain risk management. *Journal of Business Logistics*, 29(1), 133–155.
- Mena, C., Melnyk, S. A., Baghersad, M., & Zobel, C. W. (2020). Sourcing decisions under conditions of risk and resilience: A behavioral study. *Decision Sciences*, 51(4), 985–1014.
- 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.
- Mitroff, I. I., & Alpaslan, M. C. (2003). Preparing for evil. *Harvard Business Review*, 81(4), 109–115.
- Murray, B., & Bradley, S. (2021). Semiconductor chip shortage hits medtech: Strategies to build resilient supply chains. *Deloitte Health Forward Blog*. <https://www2.deloitte.com/us/en/blog/health-care-blog/2021/semiconductor-chip-shortage-hits-medtech-strategies-to-build-resilient-supply-chains.html>.
- Norman, 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.
- Olson, D. L., & Wu, D. (2010). *Enterprise risk management models*. Springer Texts in Business and Economics.
- One Network. (2020). *What is a supply chain control tower?* <https://www.onenetwork.com/supply-chain-management-solutions/supply-chain-control-towers/>.
- Paris, C., & Smith, J. (2021, September 26). Cargo piles up as California ports jostle over how to resolve delays. *The Wall Street Journal*. <https://www.wsj.com/articles/cargo-delays-are-getting-worse-but-california-ports-still-rest-on-weekends-11632648602>.
- 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., 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.
- Pfeffer, J., & Salancik, G. R. (1978). *The external control of organizations: A resource dependence perspective*. Harper & Row.
- Polyviou, M. (2016). *Essays on supply chain disruptions: A schema, managerial reactions, and decision-making*. Doctoral dissertation, The Ohio State University.
- Polyviou, M., Rungtusanatham, M. J., & Kull, T.-J. (2022). Supplier selection in the aftermath of a supply disruption and guilt: Once bitten, twice (not so) shy. *Decision Sciences*, 53(1), 28–50. <https://doi.org/10.1111/deci.12528>
- Polyviou, M., Rungtusanatham, M. J., Reczek, R. W., & Knemeyer, A. M. (2018). Supplier non-retention post disruption: What role does anger play? *Journal of Operations Management*, 61, 1–14.
- Ramasesh, R. V., & Browning, T. R. (2014). A conceptual framework for tackling knowable unknown unknowns in project management. *Journal of Operations Management*, 32(4), 190–204.
- Rao, S., & Goldsby, T. J. (2009). Supply chain risks: A review and typology. *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.
- Reimann, F., Kosmol, T., & Kaufmann, L. (2017). Responses to supplier-induced disruptions: A fuzzy-set analysis. *Journal of Supply Chain Management*, 53(4), 37–66.
- Resilinc. (2021). Supply chain disruptions- Resioinc's mid-year report. <https://www.resilinc.com/in-the-news/supply-chain-disruptions-resilincs-mid-year-report/>.
- 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.
- Sacks, C. A., Kesselheim, A. S., & Fralick, M. (2018). The shortage of normal saline in the wake of Hurricane Maria. *JAMA Internal Medicine*, 178(7), 885–886.
- Sharma, A., Adhikary, A., & Borah, S. B. (2020). Covid-19's impact on supply chain decisions: Strategic insights from NASDAQ 100 firms using Twitter data. *Journal of Business Research*, 117, 443–449.
- Sheffi, Y. (2005). *The resilient enterprise: overcoming vulnerability for competitive advantage*. MIT Press Books.
- Sheffi, Y. (2020). *The new (ab)normal: Reshaping business and supply chain strategy beyond Covid-19*. MIT CTL Media.
- 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., Schmidt, W., & Wei, Y. (2014). From superstorms to factory fires: Managing unpredictable supply-chain disruptions. *Harvard Business Review*, 92(1/2), 96–101.
- Simchi-Levi, D., Schmidt, W., Wei, Y., Zhang, P. Y., Combs, K., Ge, Y., Gusikhin, O., Sanders, M., & Zhang, D. (2015). Identifying risks and mitigating disruptions in the automotive supply chain. *Interfaces*, 45(5), 375–390.
- Smith, J. (2020, April 15). Divided supply chains are challenging producers, retailers. *The Wall Street Journal*. <https://www.wsj.com/articles/divided-supply-chains-are-challenging-producers-retailers-11586974088>.
- Smitham, E., & Glassman, A. (2021). The next pandemic could come soon and be deadlier. *Center for Global Development*. <https://www.cgdev.org/blog/the-next-pandemic-could-come-soon-and-be-deadlier>.
- Sodhi, M. S., & Tang, C. S. (2012). *Managing supply chain risk* (Vol. 172). Springer Science & Business Media.
- Suazo, M. (2011). The impact of affect and social exchange on outcomes of psychological contract breach. *Journal of Managerial Issues*, 23(2), 190–205.
- Supply Chain Risk Leadership Council (SCRLC). (2011). *Supply chain risk management best practices*. <http://www.scrcl.com/>.
- Taleb, N. N. (2007). *The black swan: The impact of the highly improbable* (Vol. 2). Random House.
- Tang, C., & Tomlin, B. (2008). The power of flexibility for mitigating supply chain risks. *International journal of production economics*, 116(1), 12–27.
- Tang, C. S. (2006). Robust strategies for mitigating supply chain disruptions. *International Journal of Logistics: Research and Applications*, 9(1), 33–45.
- The White House. (2021a, February 24). Executive order on America's supply chains. <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/>.
- The White House. (2021b, October 13). Fact Sheet: Biden Administration efforts to address bottlenecks at ports of Los Angeles and Long Beach, moving goods from ship to shelf. <https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-biden-administration-efforts-to-address-bottlenecks-at-ports-of-los-angeles-and-long-beach-moving-goods-from-ship-to-shelf/>.
- Timmermans, K., George M., & Lagunas, J. (2020). Building supply chain resilience: What to do now and next during COVID-19. *Accenture*. <https://www.accenture.com/us-en/about/company/coronavirus-supply-chain-impact>.

- Tummala, R., & Schoenherr, T. (2011). Assessing and managing risks using the supply chain risk management process. *Supply Chain Management: An International Journal*, 16(6), 474–483.
- US Department of Defense Standard Practice. (2012). *System safety*. <https://www.dau.edu/cop/armyesh/DAU%20Sponsored%20Documents/MIL-STD-882E.pdf>.
- US Department of Health and Human Services. (2020). *Strategic National Stockpile*. <https://www.phe.gov/about/sns/Pages/default.aspx>.
- Van Weele, A. J. (2010). *Purchasing & supply chain management: Analysis, strategy, planning and practice*. Cengage Learning.
- 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.
- Wiedmer, R., Rogers, Z. S., Polyviou, M., Mena, C., & Chae, S. (2021). The dark and bright sides of complexity: A dual perspective on supply network Resilience. *Journal of Business Logistics*, 42(3), 336–359.
- 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.
- World Economic Forum. (2013). *Building resilience in supply chains*. http://www3.weforum.org/docs/WEF_RRN_MO_BuildingResilienceSupplyChains_Report_2013.pdf.
- World Economic Forum. (2021). *Why disciplines must work together to prepare for future pandemics*. <https://www.weforum.org/agenda/2021/07/disciplines-together-future-pandemics/>.
- World Health Organization. (2017). Asia Pacific Strategy for Emerging Diseases and Public Health Emergencies (APSED III): Advancing implementation of the International Health Regulations (2005). Manila, Philippines. World Health Organization Regional Office for the Western Pacific; 2017. License: CC BY-NC-SA 3.0 IG. <https://iris.wpro.who.int/bitstream/handle/10665.1/13654/9789290618171-eng.pdf>.
- Wucker, M. (2016). *The gray rhino: How to recognize and act on the obvious dangers we ignore* (1st ed.). St. Martin's Press.
- Yaffe-Bellany, D., & Corkery, M. (2020, April 11). Dumped milk, smashed eggs, plowed vegetables: Food waste of the pandemic. *The New York Times*. <https://www.nytimes.com/2020/04/11/business/coronavirus-destroying-food.html>.
- Zinn, W., & Bowersox, D. J. (1988). Planning physical distribution with the principle of postponement. *Journal of Business Logistics*, 9(2), 117–136.
- Zsidisin, G. A. (2007). Business and supply chain continuity. *CAPS Research Critical Issues Report*. <https://www.capsresearch.org/library>.
- 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., & Henke, M. (2019). *Revisiting supply chain risk*. Springer Series in Supply Chain Management.
- 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.