Andrew R. Thomas · Sebastian Vaduva
Editors

Global Supply Chain Security

Emerging Topics in Research, Practice and Policy

Springer

Global Supply Chain Security

Andrew R. Thomas • Sebastian Vaduva
Editors

Global Supply Chain Security

Emerging Topics in Research, Practice and Policy

Springer

Editors
Andrew R. Thomas
University of Akron
College of Business Administration
Akron, OH, USA

Sebastian Vaduva
Emanuel University of Oradea
Oradea, Romania

ISBN 978-1-4939-2177-5 ISBN 978-1-4939-2178-2 (eBook)
DOI 10.1007/978-1-4939-2178-2
Springer New York Heidelberg Dordrecht London

Library of Congress Control Number: 2014956676

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

In 2012, President Barack Obama launched the National Strategy on Global Supply Chain Security. In addition, the US National Academies of Science, through the Transportation Research Board, created a working group of the same name. The National Strategy includes two goals:

- *To Promote Efficient and Secure Movement of Goods*
  This first goal is to promote the timely and efficient flow of legitimate commerce while protecting and securing the supply chain from exploitation and reducing its vulnerability to disruption.
- *To Foster a Resilient Supply Chain*
  The second goal is to foster a global supply chain system that is prepared for and can withstand evolving threats and hazards and that can recover rapidly from disruptions.

The global supply chain encompasses all the links connecting a manufacturer to the end users of its products. These links may take the form of manufacturing plants, supplier warehouses, vendor facilities, ports or hubs, retail warehouses or facilities, and outbound shipping centers. They also implicate all the methods and mechanisms that goods are transported: by truck, ship, airplane, or railcar. Since the inception of transportation networks, security has continuously played a role, albeit mostly a tertiary one, in the planning and execution of increased efficiencies and cost reduction.

On September 12, 2001, leaders of organizations the world over woke up to a new set of realities, more formidable and unexpected then they had ever faced. Some of the realities were subtle and even necessary: government agencies increasingly scrutinized the content of telecommunications and financial transactions. Others were stark and in-your-face: mind-numbing security lines at airports and new import/export regulations. In spite of those traumatizing events, the global economy continued to grow with even more goods, services, and people moving through the global supply chain, increasing the necessity for better understanding and security.

As the post-9/11 era is evolving, it is clear that this newly acquired friction will be part of the new supply chain reality. Organizations that had been accustomed to a steady devolution of the non-revenue-generating aspects of their enterprise like security row were now thrust into the need to somehow deal with these realities. And, while the 9/11 attacks were undoubtedly a dramatic event, they also brought security to the forefront.

When trying to secure something as vast and dynamic as the global supply chain, a lot can go wrong, including systematic mismanagement and inefficiency, criminal activity, or terrorism – to name just a few. On the other side of the ledger, government regulation, industry or association oversight, and security agencies – both public and private – remind us that there is just too much at stake to let problems languish or stagnate. It estimated, for example, that thieves now steal $80 billion in goods each year from various points along the supply chain. What's more, problems grow in magnitude when goods cross national borders, as they do with increasing frequency in the global economy.

Meanwhile, governments continue to expand security mandates deeper into global supply chains. This continues to alter the ways supply chain security is viewed by policymakers, industry, and researchers around the world. Protecting the physical infrastructure of the supply chain – along with cargo, passengers, and personnel – is now held as both a national security priority and organizational necessity. Melding two very different objectives – security for the nation and efficiency for stakeholders – poses a new challenge to those who seek to understand the changing dynamics of the global supply chain. In the United States, for example, the creation by the Federal Government of the Transportation Security Administration in 2002 threw down the gauntlet as to the importance of the issue from both a public policy and management point of view. New governmental method mandates and compliance requirements for supply chain security must become a priority for all firms, whether they agree with it or not.

Globalization, stricter security regimes, the threat of terrorism, and increasingly sophisticated criminal activity have made cross-border cargo movements more complex, putting the integrity of supply chains at much greater risk. As an executive from a global electronics manufacturer that operates in more than 150 countries put it recently, “We can have the most incredible manufacturing, but without effective global supply chain security, our products die as soon as they hit the border.”

Further, in the hypersensitive media-obsessed world of today, international and even domestic terrorists recognize the impact an attack against the global supply chain can have. As a result, much of the action around global supply chain security is being driven by the actions of those who seek to harm the system. These individuals and groups have shown remarkable resilience and no sign of backing away from the multiple targets of opportunity they perceive that the supply chain provides them. Finally, as globalization makes more inroads, the exponential expansion of the supply chain in the coming decades will ensure that the security component remains front and center.

So where do policymakers, students, scholars, and practitioners from around the world go to learn about global supply chain security? There are very few volumes

that exist in a global-centric fashion for those interested in learning more about this vital commercial component. This single volume is designed to help fill that gap and provide support to the President's National Strategy and the work of the National Academies of Science. It is our sincere hope that this work, which is written from a truly global point of view, will be one of many works going forward on this most important topic.

The chapters in this book explore the context of global supply chain security and serve as a basis for understanding the unique aspects of the innovative practices that are also found here.

In Chap. 1, Erik Hoffer, who for many years served as Chairman of Education for the International Cargo Security Counsel and later helped to develop the curriculum for the graduate program for cargo security professionals at the United States Merchant Marine Academy (USMMA), sets the stage. In Chap. 2, Captain Jon Helmick, a professor at USMMA, takes a deep dive into the evolution of maritime piracy and how it is playing out today within the global supply chain.

Then, to remind us of the multifaceted nature of our subject matter, Dr. John Harrison provides insight into how the nature of political risk shapes public policy, while Dr. Mark Beaudry details how corporate security and supply chain management can work better together.

The next four chapters further turn up the resolution. Jon Loffi, Ryan Wallace, and Edward Harris examine global supply chain security through the lens of grid and group theory. Mohammad Karimbocus rings the bell that the prism of organizational behavior must be well understood in any human endeavor. Professor Jim Bradley creatively looks at how firms might structure their capacity and inventory in ways that reduce the negative impacts of supply chain events. Charlotte Franklin and Kiersten Todt, both national leaders in emergency management and risk assessment, provide an innovative approach to making responses to supply chain events as effective as possible.

Next, Paul Alexander and David Forbes give us a fascinating look at the seafood supply chain and analyze how deliberate security breaches play a role.

As the development of the Suez Canal continues, A. O. Abd El Halim and Hussein Abbas consider its significance. And, finally, Wade Rose and Steven Murphy help us to remember Mike Tyson's adage that "Everyone has a plan 'till they get punched in the mouth." Developing a successful strategy for global supply chain security requires much more than simple planning.

On behalf of the contributors, the publisher, and ourselves, we thank you for taking a look at this volume. Please feel free to share any ideas or recommendations you may have in the spirit of collaboration with which this publication was assembled.

Akron, OH, USA — Andrew R. Thomas
Oradea, Romania — SebastianVaduva

Contents

The Context of Global Supply Chain Security

Erik Hoffer

Abstract The first goal of global supply chain security is to promote the timely and efficient flow of legitimate commerce while protecting and securing the supply chain from exploitation and reducing its vulnerability to disruption. The second goal is to foster a global supply chain system that is prepared for and can withstand evolving threats and hazards and that can recover rapidly from disruptions. To achieve this, planners will prioritize efforts to mitigate systemic vulnerabilities and refine plans to reconstitute the flow of commerce after disruptions.

Keywords Supply chain management • Criminal threats • Terrorism • Continuity planning • National security • Naval logistics

Introduction

Logistically speaking, ignorance is bliss. Most of us think that stuff just gets from one place to another seamlessly and that when we want a watermelon, it's there for us. A pair of jeans: no problem. Same goes for a computer, TV, car, and most every other want and desire we can imagine.

In fact, the notion of the seamless movement of cargo in all modalities, across the world, is really true. For the most part, at one level, with the exception of war or a terrorist attack, weather, and natural disaster areas, cargo does move from place to place rather easily. General cargo, unlike air express items, moves at a pace compatible with the modality, the length of travel, the girth and weight, the point of

Authors Note: The material in this chapter came from the dozens of seminars developed while serving as Chairman of Education for the International Cargo Security Counsel and as the curriculum developer for the Master's in Cargo Security Program at the USMMA (United States Merchant Marine Academy) at Kings Point, NY. A recommended reading section provides further resources for the reader.

E. Hoffer (✉)
Partner in CGM-NV, 24156 Yacht Club Blvd., Punta Gorda, FL, USA
e-mail: alphadog63@comcast.net

A.R. Thomas, S. Vaduva (eds.), *Global Supply Chain Security*,
DOI 10.1007/978-1-4939-2178-2_1

origin, and the degree of transport scrutiny. From what we see as consumers, the items are almost always available wherever and whenever we may wish to purchase them. Still, there is a lot happening behind the scenes, which is the basis for this introductory chapter.

The Disruptive Elements of the Global Supply Chain

There are three disruptive elements to the global supply chain that can threaten its security: natural disasters, acts of war or terrorism, and theft and domestic labor strikes or shutdowns. Each of these can be compounded and exacerbated by any of the others, and all of them can potentially occur at the same time. Further, any one of these events can bring a country or city to its knees and cause economic chaos, financial losses, or physical hardship on a national scale.

The failure to advance commerce by the movement and delivery of goods and services is the single biggest economic disruption possible in a free market and world economy. Looking at the possible ramifications from a disruption in the supply chain can send chills down the spine of any product manufacturer or service provider. From the terrorist prospective, an act of economic terrorism or, loosely translated, a weapon of mass effect is or can be more devastating than a bombing. When terrorism is involved with supply chain disruptions, the net effect achieves the goal of the perpetrator.

The lack of component products, raw materials, and processing materials, combined with no packaging and/or labor availability, can bring the economy to a screeching halt. Such is the downside of any significant disruption in our commercial supply chain. Isolated issues are the norm in viewing business planning in connection with supply chain problems. Rarely are the issues so significant, outside a war, that preclude reasonable remedy to the problem in the form of rerouting or other means of recovery. Weather is a prime example of an isolated disruptive force. Port strikes, airport closures, overseas supply chain incidents, terrorism, and many other issues typically occur in some locality and do not close down alternative routes or means to recover business operations.

Further, if we look at supply chain security through the prism of natural disasters, we can more easily accept the sudden lack of goods and the resupply concept of food, clothing, water, and basic necessities.

Take Hurricane Katrina, for example. Even with the confirmed prior knowledge of the impending storm, proper logistic protocols still were not established or preplanned. No one seemed in charge. No one created nor set in motion an action plan that involved logistics, until almost a week after the disaster! Supply lines were cut off, repairs were not readily possible, and governmental leadership at both the federal and local levels was stifled and mired in domain issues, red tape confusion, and bureaucratic turmoil. Amidst the confusion, supplies were readily available but inaccessible. Routes for vehicles, as well as some air and rail lines, were closed. Those left in the affected zone were helpless in getting the necessities they needed

for many days. 9/11 was also a tragic yet isolated supply chain issue. That event shut down airports and crippled New York City for months. Emergency procedures were installed, post 9/11, in the city that precluded the seamless entry of materials by truck and rail into the NYC area. The slowdown of materials entering the affected area was tantamount to a second disaster.

Vulnerability to our logistic system unfortunately is vast. It not only deals with the domestic supply chain, and because we are so dependent on foreign goods and raw materials, disruption abroad can cause chaos here at home as well. We have made significant strides in deterring terrorist issues that adversely affect the domestic supply chain but remain helpless in any natural disaster.

Dealing with natural disasters has always been seen as a more regional issue, where help can be brought to bear to hasten recovery, save lives, and to provide aid. Regional disasters such as tornadoes or floods are, for the most part, a known regional issue, and most areas prone to these issues are prepared. They have adequate building codes, typically appropriate and trained teams of managers and first responders available, and they are familiar with the issues surrounding these disruptions.

In acts of terrorism, however, planning must be more contingency based, which involves planning at a completely different level both here in the United States and abroad. Because of the sophistication of logistics as a science, most businesses have adopted just-in-time (JIT) philosophies on inventory and raw materials. Many larger manufacturers pride themselves in having multiple nondependent overseas suppliers, routes, and redundancy. In critical situations, it is hoped by risk planners that no two of these backup systems will fail simultaneously. Although they may have adequate distribution and storage centers, many manufacturers still rely on imported or pre-manufactured goods, arriving when and where needed to maintain production in the event of a disruption. In that business model, many disregard disruption as a part of doing business, but don't be fooled there is no complete answer and no one single silver bullet remedy to avoid all forms of supply chain problems.

Food, for example, fits that picture by necessity, and so many other manufactured and retail goods rely on JIT inventory processes to keep their factories or stores in operation. Since non-processed food is the most significant product adversely affected by a supply chain disaster, retailers are powerless to recover when food is their main product. Besides quickly using up staged food products, no one can remanufacture it! Logistical remedies are not typically applicable to the recovery of these products; hence, supply chain disruption instantly, and adversely, affects the costs of food products regionally and even at times nationally based on the origin, location, and magnitude of the disruption. Issues such as a strike or road closure can cause food to be unnecessarily and possibly inappropriately stored. The fact that storage conditions can adversely affect the efficacy of pharmaceuticals, cause food to rot, and create lag times in further processing is also a major set of vulnerabilities when providing risk-based planning for manufacturers.

Insurance has always been the go-to answer for problems in the supply chain. To say "no worries, I'm insured" used to be a viable and at times successful remedy, however, not so today. More insurance providers require special coverages for each potential mishap in the supply chain. These special insurance conditions rely on a

crystal ball analysis of the "could-be" possibilities of supply chain issues. Needless to say, one could never predetermine what may happen to the goods in transit; hence, protection methodology such as insurance rarely is a viable or effective remedy to supply chain losses.

The Scope of the Global Supply Chain

The commercial supply chain incorporates all transit modalities. Goods of all kinds move by truck, rail, sea, including barges, and air and often in combination among these methods. The commercial supply chain is affected by any condition that causes delays in moving people and materials. It has hundreds if not thousands of internal operating elements comprised of logistic companies and their physical assets, local and national governments, laws, tariffs, and energy and fuel providers. Millions of people and infrastructure including roads, bridges and tunnels, rail, waterways, ports, airports, and rail lines all are required to work in concert to create the supply chain. The international supply chain is the backbone of business and the heart of the world's economy. Our domestic supply chain affects the world market, the financial stability of many countries, the ability of our armed forces to function, and our national economic stability. It is the single most important element of any country, because without it, everything comes to a screeching halt. Each and every factor from a country's ability to function to its economic core relies on a functioning commercial supply chain.

During each day, somewhere around 38 million major cargo shipments and 75 million courier shipments begin and end at our doorstep. At the same time, well in excess of 50 million commercial cargo shipments begin and end in this country each and every day.

As consumers, we take in air cargo as a matter of course and welcome the couriers and drivers as they deliver products to us. Little consideration is given to most of this cargo, specifically, where it has been, who handled it, who shipped it, is this the same generic box that was tendered to the courier, or the fact of the relative safety of its contents. We just sign the form and take it in! The same goes for companies whose shipment is considerably larger and whose items typically move by truck, yet the system is the same and the complacency toward receiving materials is replicated everywhere.

Air cargo, truck cargo, and containerized freight are neither safe nor secure while they are in transit. In most cases, the contents are implicitly safe but there are no guaranties. Typically, what people say is in the box is recorded as such and accepted. Cargo or small packages tendered to commercial airlines at counters do get screened, but at what level as compared to baggage or palletized cargo?

Speed is both the benefit and risk of air cargo! Air cargo, as compared to all conventional forms of transit, gets its greatest security boost from delivery speed, but anonymity of the true contents is the risk. The supply chain for air cargo also incorporates the cold chain system where millions of time- and temperature-sensitive

items move worldwide daily, each with the critical element of speed being the factor which determines the need for air freight.

Air cargo rarely sits still. Cargo at rest becomes cargo at risk from a storage and theft prospective. Any logistician knows that vulnerability, but yet air cargo gets far less scrutiny than we would like to insure its integrity, both aboard commercial aircraft as well as air cargo freighter aircraft. Inbond facilities are notoriously suspect for true long- or short-term containment or control thereby placing another bug in the seamless supply chain. The known shipper program, as it relates to bulk air freight, has begun to identify consistent air cargo shippers, and it has radically and positively contributed to air cargo integrity and security. Serious delays can result for shippers who are unknown or noncompliant with new air shipping regulations.

This risk of delay or theft and the subsequent possibility of loss for air shipments should be a focused area of concern for all corporations. Government regulators, in an effort to secure our supply chain, have created hundreds of new laws and requirements on air freight which, if a shipper is unfamiliar with them, will delay and disrupt what would otherwise be a fast and secure method of transport. Everyone dealing with air freight or courier cargo needs to establish a transfer inspection protocol to insure the goods are actually being moved and not stuck in a warehouse or a customs facility because of documentation or other glitches in paperwork. The risks of a significant supply chain disruptive event, by air cargo, are enhanced by world events. They are not limited to bombs but rather to the gambit of possible problems, which include bioterrorism, drug traffic piggybacked in your containers or courier packs, and cargo pilferage. Each event, regardless of location, can shut down the air freight system, worldwide. Any event can be the basis of shutting down your supply chain without notice.

Domestic truck and rail shipments also pose an equally serious problem should a domestic or foreign disaster issue stifle the ability to move freight. Whether that problem is across state borders or across the world, the commercial supply chain will suffer until remedy can be found and implemented. In fact, no modality is risk free, and since all logistic operations involve some choice in the mode of delivery, the supply chain becomes the single greatest economic target for terrorism.

The Concept of Global Supply Chain Security

Supply chain security is more of a concept than a condition. No one can foresee unexpected disruptions nor can they be planned for. The precariousness of loss free shipping has always been part of the logistic planning function, but with today's manufacturing being more often JIT by nature, logistic losses and delivery disruptions play a far bigger role in the effectiveness of a company's profitability than ever before. Vulnerability for loss is a constant threat to any cargo, whether attended or unattended, monitored or not. Proper planning prevents the obvious conditions such as weather-related issues, suspect route choices, weekend moves, or storage or basic damage issues. But true supply chain security needs to be a coordinated effort among shippers and carriers and in a way must also rely on just luck.

The commercial supply chain is no more secure today than 20 years ago. The dynamics have changes and yet the processes of protection have not. Moreover, supply chain disruptions occur because most shippers and carriers fail to dedicate the proper resources to loss mitigation at the outset so as to reduce risk through technology. One of the technologies adopted to track cargo and the vehicles that move it is called telematics. It is more for equipment efficiency than security, more as a real-time logistic planning tool than for loss control, and surely oriented more toward the carrier than protecting the products or the shipper. Collaterally, shippers benefit from speed, better routing, and up-to-date information on loads, but statistically, losses in theft have remained a constant for the last 35 years and other losses in the supply chain are rarely remedied by these instruments. Theft losses, for example, in the domestic commercial supply chain average more than $20 billion annually, but the caveat here is in understanding losses and their ramifications which make that figure grow 8–10 times. Theft losses are a known condition. Many companies tolerate as much as 3 % of their gross annual sales through theft-related losses. Other commercial supply chain losses through other conditions seem to be unplanned for and therefore do not hit the balance sheet as anything other than write-offs. Theft, of all the perils to shipped cargo, is the only known condition of loss that you can count on as a corporate bean counter.

Losses through supply chain anomalies are never limited to the tangible product itself. The inability of the seller to replace the goods to the buyers in a timely fashion, combined with the logistic, insurance, and administrative costs of the loss, makes the issue of theft, damage, delay, or disappearance a far great detriment to the economy than one may see at the surface. Once you recognize that the loss is not limited to the seller, you can see why clients have to hedge their bets when goods go missing or are delayed. The inability to manufacture a product because of stolen or missing components reeks havoc with global supply costing millions in labor and creating logistic nightmares in replacing it. When goods are not manufactured on time, they cannot be shipped. However, boats and planes don't wait, and therefore, cargo losses mount exponentially.

Brand equity is a constant problem with supply chain disruptions. Lost, damaged, or stolen goods quickly appear on global markets, in Internet sales companies, and at flea markets, worldwide. For example, losses of goods from anything from an earthquake to a super storm are going to be recovered by someone. That someone will then own the goods in question. That new owner can be an insurer, a salvage company, or anyone for that matter. Once recovered and now re-homed, these goods can be sold again in direct competition to the original owner. No longer can the original owner control his brand, his sell price, his distributors, or any other factor indigenous to his business. The loss of a retailer's margins and a brand owner's ability to control his supply chain, based on these goods being recovered or free astray in the market or stolen and now having a zero cost base, makes for tremendous losses for all concerned.

Recovery costs are also a concern. Many companies employ security personnel on a global scale to attempt to recover lost or stolen goods; however, they are rarely successful. Even if by chance they do stumble on a truckload of a product, its return

to the market becomes precarious and costly. If it is a product that is now out of season or date, recovery is almost meaningless because the item cannot be resold. If the item is an ingestible, recovery means a complete reversal of insurance payments, if any existed, causing the company a second compounded loss of revenue.

The Likelihood of Global Supply Chain Disruptions

Most people can come up with their own personal scenarios on disasters, which disrupt the global supply chain be they man made or natural. If you put 100 people in a room and ask them for three ways they could disrupt life as we know it, you will likely get 300 quality scenarios. Given that these folks probably have never had such ideas beforehand nor would they ever consider acting on them, you can only imagine what terrorists could conceive of. Supply chain disruptions or, as mentioned, these weapons of mass effect are extremely dangerous and possible. Because threats to national security are ever-present, our government has taken steps which they feel would best serve to deter the bulk of the most simple and common issues and thereby focus on the percentage of issues that are not only more sinister but require a more dynamic plan and more people to carry it out. Natural disasters need no such sophistication and can happen anywhere and at any time.

The global supply chain takes into account far more elements than simple domestic logistics. Countries have varying degrees of sophistication in all areas of transportation and consequently differ in efficiency, preparedness, adaptability to issues, and transport options in the event of a disruption. Customs processes and local laws affect supply chain dynamics. Based on their degree of implementation, corruption, and sophistication, goods can spend inordinate amounts of time being processed, inspected, or scrutinized or simply be passed through willy-nilly.

The Local Approach to a Global Issue

From the borders of African nations and Middle Eastern nations to the volume of goods from the EU and China, products travel in very different ways, with totally different documentation, protection, inspection, and efficiency. There is no global road map for supply chain security, and there is surely no consistency. From the natural disaster prospective, what happens in the smallest country can bring a world economy to a screeching halt.

Countries adapt to their surroundings and cultures. The nature of supply chain consistency and security on a global scale is haphazard and relies on basic business principles to work. A small country whose supply lines act as a choke point to other countries or critical ports can create a nightmare if that country has no funds or the ability to repair roads, bridges, tunnels, or ports based on the nature of the disaster. International aid can take weeks thereby causing irreparable harm downstream.

In the United States, the Department of Homeland Security (DHS), Immigration Customs Enforcement (ICE), and many other agencies have some role in protecting the nation by overseeing the global supply chain. Their orientation however is physical security. These agencies could care less, by design, that one company's cargo is being held for a container screen, or the ship carrying a company's cargo is being delayed coming into port due to some contraband being found on board. Disruptions can come at anytime and anywhere, caused by the laws designed to protect us! That help provided by national policy to protect us can be counterproductive to the supply chain. Additionally, supply chain disruptions outside the United States based on counterterrorism vary drastically. These efforts, through having a common core, are also frequently the cause of cargo delays.

Programs have been established at tremendous costs to both the government and industry and still do not address the problem globally, leaving us almost as vulnerable as without their implementation. Many of these laws focus on air and sea transportation, while others shore up our borders against over the road issues. Some of these programs include C-TPAT (the Customs-Trade Partnership Against Terrorism), TWIX, BASC, and Known Shipper, but these types of programs are now worldwide and some are stronger yet many are weaker but none are the same or seamless. Shipping worldwide has become far more difficult and complex since 9/11.

Each new law for protection against terrorism addresses what we cannot control through our own logistical processes and personnel, yet since each country has a different set of standards, shipping goods can be more costly and more complex. As an example, if a company has a specific pallet they use to ship goods from their suppliers, because it fits their mechanized system, they need to be certain that the origin countries allow for that size or pallet material is permitted. China, for instance, does not allow certain woods to be used as pallets. A shipment of baby powder from a plant in Columbia would get through their customs with simple documentation and land in the Port of Newark by ship in a few weeks time. Once it arrives, however, the anomalies of powder shipped by sea freight coming from Columbia would trigger vast inspections at high costs and with radical delays. It would then be off loaded and moved by truck to an inspection plant and would require special oversight to be released. A shipment of the same goods from a facility in New Jersey traveling to Mexico, for instance, would be screened, inspected, and approved at least three times before it crossed the border thereby making it easier to export the material than to import it.

The Notion of Vulnerability

The vulnerability of our supply chain is vast, and yet the reliability and resilience of it exceed that of any other country. It seems that in spite of Mother Nature's wrath, and notwithstanding the possibility of another terrorist incident or theft, we seem to pull out all of the stops to return ourselves to life as usual and achieve normalcy quickly and efficiently.

Is the global supply chain as secure as it could be? Have we planned for all of the potential disruptions? What can we do to improve our ability to recover from supply chain problems, and what are the commercial and governmental ramifications of longer-term supply chain interruptions?

These are all questions that every company and government must answer. Whether they are manufacturing, importing, or exporting, regardless of modality or supply speed and regardless of the nature of the goods shipped or received, supply chain disruption planning is mandatory as a planning tool. The paradigm of ignorance is bliss has no place in logistical planning.

The nation's road system is both a federal and state responsibility. When issues threaten the viability of the road system, for example, action needs to be generated in such a manner that repairs are effectuated within reasonable time frames. Empirically, this concept seems logical and workable. However, as we have seen time and time again with natural disasters, confusion becomes more of the rule then anyone would prefer. Ownership of the responsibility can only work if planning has already taken place wherein each party knows their responsibility and each party, including local, state, and federal, has the infrastructure and resources in place to address the problem.

Our roadway system is the single most vulnerable entity in the supply chain, and it goes without saying that any disruption to it, anywhere in the nation, can dramatically and exponentially affect the nation as a whole. Because the Federal Interstate Highway System has no real form of protection, it is easy to see where any breach can slow down or shut down vast sections of the country dependent on that particular route.

Savvy logisticians consider supply chain routes in planning materials movement. Many truckers also evaluate route and distances for both cost savings and against vulnerabilities such as hijacking, theft, stopover points, drop trailer lots, and driver distances to mention a few considerations. Most shippers fail to consider these vulnerability components, while truckers and third party providers rarely look at supply and resupply issues in the event of a catastrophic event. The combination of initial supply and resupply is tantamount to a total supply chain plan.

There are no quick fixes for downed bridges, highway roadway surfaces, and tunnels. These fixes require time, and time is the logistician's enemy. Because of this, many security and safety recommendations by the federal government have been proposed, but few actually have been implemented and even less have become law.

Regardless of the supply disruption, the downside of the failure of any infrastructure element wreaks economic havoc on a national scale. Repairing such a problem also presents a formidable challenge. Rerouting changes the delicate balance of major and minor roadways, it disrupts traffic patterns causing even more burdens on smaller communities, and of course it increases operational costs at every level. The time it takes to repair roadway issues and the burden of cost taxes the ability of the states affected in a myriad of ways. If the disruption was terrorist based, repairs may be a far more arduous task since there may be more involved with security than with a natural disaster. The elements of the state and federal government charged with repair can also vary where funding and resource allocation may be concerned.

Approaching Global Supply Chain Security Vulnerability

Businesses whose processes involve shipping and receiving goods through every modality, and those who provide the logistic services, need to coordinate and explore both short- and long-term fixes when and if a disruption does occur. In most cases, these discussions are met with tremendous resistance by all concerned, as there are no fixes that don't involve unseen expenses, major changes in operations, dedicated personnel, and higher costs. Backup plans, however, are far less costly when documented in advance, practiced, and funded and accepted as a cost of doing business on a large scale.

Supply chain disruptions can be couched as an expense or as a component of manufactured costs. Backup materials vs. JIT supplies can almost be seamless in certain operations where there are contracted buffer storage facilities available, where multiple shipments are scheduled in at a faster pace for seasonal production, or where more on-site inventory is acceptable. Of course, certain operations do not lend themselves to these alternatives, and, therefore, these businesses will be far more negatively affected by any supply chain disruption.

Globally, terrorism is a real and omnipresent way of life. The instability in the world increases daily where there is little remedy and even less deterrence. Our government and most of the world's governments have seen these issues first hand. Each has unto themselves proposed and adopted a plan of addressing both deterrence and recovery, yet each plan on the world stage is still disjointed. In many cases, these plans are unrealistic for the country to implement and uncoordinated among other trading partners leaving undetected and inherent weaknesses to the world supply chain in direct opposition to the core idea of security.

The United States created numerous agencies and internal departments to address infrastructure recovery and basic supply chain security. These groups now account for 500,000 new employees, doing their interpretation of the overall mandate. It is difficult to determine how the lines are drawn since overlap is the nature of protection. Agencies such as ICE, DOE, DOS, and DHS and the FBI, SS, NSA, and CIA all have their fingers in the pie, yet coordination between them is sparse and at times nonexistent. Laws have been passed that give each partner certain mandates such as the creation of the CCSP by DHS, the TSA also by DHS, the Patriot Act, and the C-TPAT. Many of these laws and recommended best practices have become more burdensome on businesses than effective preventative measures. Business needs an equilibrium between security and expedited movement of cargo, yet government requires consistency regardless of the effectiveness of the practice. These two conflicting paradigms provide the basis for ineffective and cumbersome requirements that are now unfortunately crucial elements of business logistical planning.

The instability in the world has spawned new business opportunities in security globally. Millions of people in almost every developed country are now dedicated to inspecting cargo, passengers, trucks, trailers, sea containers, and ports. Governments have developed new agencies, manned by untold thousands of personnel, whose job is to monitor cargo, develop new documentation, secure border crossings, oversee

warehousing and drop lot operations, and many other ancillary functions needed to close the loop against terrorist issues. The regulatory functions needed to develop and monitor systems used to protect the supply chain and commercial travel have their own bureaucratic challenges. This is a new global concept, and therefore, it runs in the face of each nation's beliefs, assessments of risk, and fiscal ability to fund, carry out, and enforce the functions created independent of one another. Although terrorism has raised the awareness of the possibility of economic collapse on a global scale, many countries are just incapable of participating in the remedy, which renders the entire system vulnerable.

Planning for Supply Chain Disruption

Planning for supply chain disruption is by no means easy. The smallest issue can be devastating to a business. Many companies however fail miserably to have even basic contingency plans in place when problems arise. Even relatively simple issues quickly become encumbered by the lack of preprogrammed remedial actions needed to address the problem. As a basis of operating a global corporation, every company should have a crisis management team which is made of empowered personnel. This team should be well organized and funded and should be in place and well practiced in order to be effective in the face of an emergency. Many national companies, even today, fail to actually have such a functioning system in place. In order to have your best chance of minimizing recovery costs, preparation and true risk management must be at play. This team should have appropriate personnel in place that span the gambit of all functional business operations and the bandwidth to unite in the face of a crisis from global points by some preplanned communication method. From human resources to supply chain assets, from logistics to physical property and inventory, and from quality assurance to manufacturing, no sector of business can be left out of the recovery equation. No business can recover from a massive disruption without all aspects of the business's operations being in the loop.

Planning is a key component in any business. Updating planned efforts that change with the times and nature of business operations makes these refined plans even more effective. Whether you are a manufacturer or a service provider, you need to be able to sustain operations, seamlessly, when these disruptions arise. Inventory levels provide some ability to limp though disasters, but most companies today work on very tight inventory programs and in most cases these buffers are only a short-term fix. While most clients understand when operations go down, they too may have backup plans that do not include your company's ability to recover but rather immediately switch business to your competitors. Regional operations with multiple common manufacturing locations typically fair the best in major disasters or disruption issues as materials and production can be switched from plant to plant. Single-source operations, which account for the vast majority of manufacturers and distributors, bear the brunt of losses due to supply chain problems.

Because the costs of losses can be so significant to a business, developing a metric-based allocation system is a great idea for logisticians. This matrix must include basic and future costs of loss while accounting for immediate- and long-term remediation and recovery costs. Because there are hundreds of categories of these costs in any business operation, placing them in order of significance is a daunting task. Each business is unique but certain tenants of operation are common, and these tend to be the first to be addressed. No business can operate without its human resources; hence, having people on- or off-site is a key element of recovery. Physical manufacturing or distribution locations tend to be high on the priority list as well, since without a location with which to operate, not much gets accomplished. Infrastructure is also a key element, but in many cases, once a disaster has happened, getting power, fuel, phone, and Net services is often out of your control. Materials, records, computer backup for operations, and machinery also round out the recovery plan.

Taken as separate components, each of these elements has their own inherent and independent issues. Taken as a business entity, their collective interaction provides the list and the ordering of recovery priorities. No list is ever stagnant, and no order of priority can exist without first having the disruption identified in order to determine what's working and needed and what's not. The supply chain is delicate. A trucking or port strike, for instance, can back up shipments, reduce available manufacturing components, and bring a business to its knees without affecting a company's ability to manufacture or perform their service. Disruptions overseas ranging from acts of terror to strikes can affect certain areas of the world without notice. Wars can create tremendous demand for certain goods which is clearly the opposite effect but no less traumatic to the supply chain.

Keep in mind that management serves both the day to day and the planning function for a business. Without both being addressed, management is not accomplishing their mission and therefore weakens the long-term prospects of the company.

The supply chain today has really not changed that much in the past 20 years. This takes into account roads, ports, rail, barge, and air transportation. We have somewhat more regulation geared toward security in place, somewhat more physical scrutiny for cargo, and somewhat better infrastructure, and yet not much has changed with regard to reducing or eliminating risk. Risk is not mitigated by insurance because, realistically, one cannot ever fully recover a loss. Risk is reduced by planning but, because of the dynamic set of possibilities, only to a small degree. Risk is an ever-present condition, and yet threat assessment is typically a second rate business function.

The Rising Importance of Security Within the Enterprise

In the recent past, security departmental functions in major corporations have morphed from having a greater say in operational planning to a role of physical (on-site) monitoring. The function has moved from a corporate line function to a dotted line from human resources. This seems to exclude the practical nature of having a security department in the first place much less a true risk management group!

Security in a corporate sense used to be comprised of physical on-site security, meaning gates, employee vetting and screening, lots, facilities, guards, and access controls. Next came issues of theft, industrial espionage, counterfeiting, diversion, product recovery, logistic oversight, and protection. Finally, security played a consultative role in business disaster planning and risk assessment. The use of these talented individuals seems to have all but disappeared, and it seems this is due to a misunderstanding of their cost vs. their benefit to business health. Without some basis in threat assessment, planning for supply chain disruptions is more of a guess than a metric- and expertise-based function.

Logistics is the only element in a business where secondary planning can be useless as a remedy because with no way to move goods in or out the business is at a standstill. Materials in any product business must be turned. Products must be able to get to their destination in a timely and safe manner, and without this logistic cycle, no sales can be recorded, nor profits made, nor clients satisfied, nor personnel working. Without a means to accomplish the mission of a business, there simply is no business.

Military Logistics as a Role Model

The challenge of planning for the unknown is daunting but possible when you prioritize issues and have the resources and flexibility to respond to sudden unpredictable situations. Once such place where supply chain disruption is the norm is military logistics. In the world of the warrior, nothing is fixed and nothing is out of the question. Military logistics is by definition the backbone of any military strategy. Without supplies, a military action ceases to function. Without contingency, planning response times become life and death situations. Unlike corporate logistics, military logistics utilizes all modalities and then inter-disperses them, at a moment's notice based on real-time issues. Unlike in the corporate world where all moves are subject to conditions, vendors, and costs, military moves are rapid responses. Unlike in the corporate world where a container of goods may in fact be the only one of its kind in the supply chain, military cargo must, by its nature, have double and triple redundancy in order to insure mission compliance. Items such as uniforms, ammunition, food, vehicles, and medical supplies must be able to be deployed wherever in the world they are needed. Military planning allows for dozens of contingencies and does not rely on one's ability to pay to have items remade or moved when and where needed. The world of military manufacturing and logistics is the epitome of disaster planning.

Besides being dynamic, military logistics is also disjointed. There are multiple branches of the military, intelligence community and defense contractors. Each element has its own mission and each typically has its own logistic operation. Many times, missions overlap as in a war or conflict zone, but many of these day to day operations are focused on that branch of service and their unique operation and asset base. The nature of the needs of the military is indigenous to each branch and even down to each operation in any theater worldwide. Let's face it, the Navy does not

wear Army uniforms nor do they need the same ammunition or employ the same tactical assets. Suffice it to say that moving supplies of every category and description into a military theater is a tremendously complex operation. If we in the corporate world think we have vulnerabilities and supply chain disruption, well think again! As compared to military logistics, even the worst disaster is a walk in the park when you are fighting a war.

More so than any corporate function, defense asset logistic needs trump any possible contingency ever encountered by any business.

Like businesses, defense-based assets need to be where they are supposed to be when they are needed. Delays in receiving assets can cost lives, and the importance of accuracy and reliability of the supply chain is crucial. Businesses have different requirements that to them equate to life or death situations. Goods delayed by supply chain disruptions can become obsolete or unusable based on the commodity and the amount of time required to complete the move. Cargo that is stagnant requires special protection. Temperature-controlled cargo requires monitoring, and in many cases, trailers or rail cars left in staging areas can become vulnerable to theft and damage.

There was a time, not so long ago, that we just didn't seem to worry about supply chain disruptions. It was not that we were invincible but rather naïve. We had plenty of materials in the pipeline, we made the vast majority of goods here in the United States, and we really didn't concern ourselves with disruptions other than those occurring naturally. In today's reality, we have a variety of concerns above and beyond what was considered the vulnerability of the supply chain. Here to for issues such as domestic and foreign terrorism were not considered eminent. Issues involving cargo theft was alive and well but considered immaterial to the normal operations of business and even the government. With an excess of 25 billion dollars stolen annually back then and even now, the focus and the understanding of its effect has only recently been a topic worthy of the board rooms.

Supply chain disruptions can involve any condition that creates a void in the supply chain, and since each disruption adversely affects other aspects of logistics, even the smallest glitch can have a major impact downstream.

A Five-Step Process for Asset Recovery Calculations

When doing disaster planning, the steps and considerations mentioned below will tend to focus you on the right track.

The Five-Step Process

1. Identify risk exposure.
2. Measure risk with known metrics and intelligence estimates based on the probability of the occurrence. Consider the financial impact of the loss and evaluate protection costs based on the ability to predict or deter the occurrence.
3. Consider how your business continuity plan enables you to recover after the loss or supply chain disaster and decide on the most appropriate defense.

4. Fund and implement solutions in their order of importance.
5. Monitor and measure the effectiveness of your planned solutions and update them over time.

Knowledge has always been the key to business continuity. If you know your business, you understand your threats to profitability, and your corporate culture permits contribution by all affected business components, you will find the road to recover after a significant disruption to your supply chain easier and less painful than "on-site planning." No one can foresee supply chain incidents such as naturally occurring events or terrorism, but you can develop and refine a plan for remedy in the event of some such occurrence.

Recommended Reading

Becker J, Delfmann P, Knackstedt R (2007) Adaptive reference modeling: integrating configurative and generic adaptation techniques for information models. In: Becker J, Delfmann P (eds) Reference modeling – efficient information systems design through reuse of information models. Physica, Heidelberg, pp 27–58

Gordhan P (2007) Customs in the 21st century. World Cust J 1(1):49–54

Gulledge T, Chavusholu T (2008) Automating the construction of supply chain key performance indicators. Ind Manag Data Syst 108(6):750–774. doi:10.1108/02635570810883996

Gutierrez X, Hintsa J (2006) Voluntary supply chain security programs: a systematic comparison. In: Proceedings of the international conference on information systems, logistics and supply chain (ils 2006), Lyon

Hellingrath B (1999) SCOR und CPFR: standards für die supply chain. Logistik Heute 21(7–8): 77–85

Hellingrath B, Laakmann F, Nayabi K (2003) Auswahl und Einführung von SCMSoftwaresystemen: Strategien und Entwicklungstendenzen in Spitzenunternehmen. In: Beckmann H (ed) Supply chain management. Springer, Berlin/Heidelberg, pp 99–122

Hintsa J (2010) A comprehensive framework for analysis and design of supply chain security standards. J Transp Secur 3(2):105–125. doi:10.1007/s12198-010-0042-3

Kannegiesser M (2008) Value chain management in the chemical industry: global value chain planning of commodities. Physical, Heidelberg

Kaufmann L (2002) Purchasing and supply management – a conceptual framework. In: Kaufmann L, Hahn D (eds) Handbuch industrielles beschaffungsmanagement: internationale konzepte, innovative instrumente, aktuelle praxisbeispiele. Gabler, Wiesbaden, pp 3–33

Lambert DM, García-Dastugue SJ, Croxton KL (2005) An evaluation of process-oriented supply chain management frameworks. J Bus Logist 26(1):25–51

Li L, Su Q, Chen X (2011) Ensuring supply chain quality performance through applying the SCOR model. Int J Prod Res 49(1):33–57. doi:10.1080/00207543.2010.508934

Mentzer JT, DeWitt W, Keebler JS, Min S, Nix NW, Smith CD, Zacharia ZG (2001) Defining supply chain management. J Bus Logist 22(2):16–28

Mikuriya K (2007) Supply chain security: the customs community's response. World Cust J 1(2): 51–59

Maritime Piracy and the Supply Chain

Jon S. Helmick

Abstract The scourge of modern maritime piracy is expensive for the international community, ocean carriers, insurance companies, and other entities that participate in and benefit from global trade. This chapter surveys the nature and scope of modern maritime piracy, summarizes the key impacts and costs of piracy for global supply chain operations, and discusses strategies that can be employed to evade, deter, and mitigate this threat. Implications of piracy and armed robbery for supply chain partners include seafarer abuse, injury, or death; the need for premium crew compensation; the payment of hostage ransoms; elevated insurance premiums; delayed cargo delivery; reduced cargo value; higher fuel costs; security equipment expenses; and the need for embarked security teams. Strategies that can be used to address the threat of piracy that are discussed include the implementation of Best Management Practices; enhanced training, drills, and exercises; naval intervention; the use of transit corridors and group transits; and supply chain reconfiguration.

Keywords Piracy • Maritime • Security • Supply chain

> 29.04.2014: 1931 UTC: Posn [Position]: 04:56N – 004:49E, Around 35 nm [nautical miles] West of Bayelsa Province Coast, Nigeria.
>
> Two armed pirates boarded a product tanker underway. As the crew retreated into the citadel the on board armed team fired at the pirates. Most of the crew including the guards managed to retreat into the citadel. Head count in the citadel indicated two crew missing. When the guards and crew emerged from the citadel they found the C/E [Chief Engineer] had been killed and the 3/O [Third Officer] with injuries. The vessel headed towards Lagos.
>
> (IMB 2014a)

The opinions expressed in this chapter are those of the author alone and do not necessarily represent the views of the US Department of Transportation, the Maritime Administration, or the US Merchant Marine Academy.

J.S. Helmick, USMS., Ph.D. (✉)
Maritime Logistics and Security Program, United States Merchant Marine Academy,
300 Steamboat Road, Kings Point, NY 11024-1699, USA
e-mail: helmickj@usmma.edu

A.R. Thomas, S. Vaduva (eds.), *Global Supply Chain Security*,
DOI 10.1007/978-1-4939-2178-2_2

Introduction

Global supply chains involving ocean shipping generally provide low-cost, efficient, and reliable long-distance transportation of commodities and merchandise. The movement by sea of high-value goods today usually accounts for less than two or three percent of sale price. In contrast to the days of sail, when vessels might take months to make an ocean crossing in unfavorable weather and arrival time was highly variable, cargo carriage by modern steam or diesel-powered ships is fast and quite predictable. Satellite-based navigation systems, electronic chart displays, computerized cargo stowage planning, software-based weather routing, automated engine room operations, and a long list of similar technological innovations characterize the operation of today's merchant ships.

It is ironic that this sophisticated maritime freight delivery system can be disrupted by a few armed men in small boats who board and rob or hijack merchant ships and hold them, their crews, and cargoes for ransom. Modern maritime piracy imposes significant costs and delays on those global supply chains that have the misfortune to become entangled in its depredations. It also represents an important economic burden for the international economy.

This chapter discusses the nature and scope of modern maritime piracy, summarizes the major impacts and costs of piracy for global supply chains, and discusses strategies that can be employed to evade, deter, and mitigate this threat.

Dimensions and Scope of Modern Piracy

Definitions

"Piracy" is defined in article 101 of the 1982 United Nations Convention on the Law of the Sea (UNCLOS) as follows:

Piracy consists of any of the following acts:

(a) Any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed:

  (i) On the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft;
  (ii) Against a ship, aircraft, persons or property in a place outside the jurisdiction of any State;

(b) Any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making it a pirate ship or aircraft;
(c) Any act inciting or of intentionally facilitating an act described in sub-paragraph (a) or (b).

The term "high seas" in international and maritime law generally refers to areas outside the national jurisdiction of coastal states. For littoral countries that claim an exclusive economic zone (EEZ), limited national jurisdiction may extend up to 200 miles off the coastline. However, the provisions of UNCLOS concerning piracy are held to include the EEZ beyond a state's territorial waters (IMO 2011).

An attack on a merchant ship that takes place inside the territorial or internal waters of a coastal state may thus be termed "armed robbery" or "maritime crime," rather than "piracy," depending on the entity that is compiling or reporting statistics on such incidents.

The International Maritime Organization (IMO) defines armed robbery as follows:

"Armed robbery against ships" means any of the following acts:

1. Any illegal act of violence or detention or any act of depredation, or threat thereof, other than an act of piracy, committed for private ends and directed against a ship or against persons or property on board such a ship, within a State's internal waters, archipelagic waters and territorial sea;
2. Any act of inciting or of intentionally facilitating an act described above.

This distinction between piracy and armed robbery based on the location of the activity complicates both the reporting and the prosecution of maritime piracy. However, because most attack statistics do not distinguish piracy from armed robbery based on the definitions above, this chapter conjoins these acts for purposes of discussion.

Incident Statistics

According to the International Maritime Bureau of the International Chamber of Commerce, there were 264 pirate attacks reported worldwide in 2013. This figure represents a decrease of 40 % relative to 2011. In 2013, the geographic area in which the greatest number of attacks took place was Indonesia. Attacks in this location totaled 106, representing a dramatic increase over the 15 such incidents reported in 2009. However, most of these incidents are termed "opportunistic theft" and must be distinguished from the much more serious type of hijacking that characterizes piracy off the African coasts (IMB 2014b).

So-called Somali piracy, involving attacks on vessels transiting the Gulf of Aden, Red Sea, Arabian Sea, off Oman, and in the Western Indian Ocean, has captured the attention of the maritime industry in recent years. The brazen and aggressive hijacking of merchant ships and the holding of their crews for ransom reached a peak in late 2010, when almost 700 mariners were being held off the coast of Somalia aboard 30 merchant ships. The phenomenon of Somali piracy was highlighted for the general public with the 2013 release of the film "Captain Phillips," which portrayed the story of the *MV Maersk Alabama* hijacking.

As a result of the combined effect of interventions discussed later in this chapter, Somali piracy has now dramatically declined. In 2013, there were a reported 23 attacks on commercial vessels, none of which were successful. At the same time, there has been a surge in the number of attempted and completed piracy attacks on vessels along the West African coast. There were an estimated 100 such incidents in 2013. Attacks in the West African region are generally more violent than those undertaken by Somali pirates (Madsen et al. 2014).

During the first quarter of 2014, maritime piracy incident statistics indicate that there were 22 attacks in the Gulf of Guinea/West Africa region, 15 attacks in the Horn of Africa/Western Indian Ocean region, and 31 such events in the waters off Southeast Asia (MAREX 2014).

There are several concerns regarding the accuracy of the statistics cited. Vessel owners and ship masters may be reluctant to report attacks to authorities. The ensuing investigation may delay the ship, which is highly undesirable from a commercial standpoint. Also, publicity concerning pirate attacks is generally considered detrimental by ocean carriers. It is variously estimated that 50–70 % of pirate attacks may go unreported.

Conversely, there are documented instances in which approaching fishing boats have been mistakenly identified as pirate craft. At the least, these occurrences result in inflation of the numbers of attempted attacks reported. Such cases of mistaken identity can have much more serious consequences. In February 2012, about 20 miles off the coast of Kerala, India, Italian marines shot and killed two unarmed Indian fisherman in a small boat as it approached the tanker *Enrica Lexie* (Banerji and Jose 2013).

Types of Vessels Targeted

Data for 2013 show that the type of ship most frequently attacked by pirates was the chemical/product tanker. There were 82 attacks reported involving this kind of vessel. The second most frequently targeted vessel type was the bulk carrier, with a total of 53 attacks. Tankers were the third most often vessel type victimized, with 39 reported attacks. Container ships were the subject of 30 reported attacks by pirates worldwide in 2013 (IMB 2014b).

Operating and design characteristics that predispose ships to being targeted by pirates include their freeboard (height of the deck above the waterline) and speed. Ships with low freeboard make it relatively easy for pirates to gain access to the deck. Similarly, vessels that steam at less than 15 knots (about 17 miles per hour) provide much less challenge for pirate boardings than do faster ships. These two factors combine to make a ship particularly vulnerable to piracy and armed robbery. In the industry, such vessels are termed “low and slow.”

Pirates have been known to make use of the internationally mandated Automatic Identification System (AIS) carried aboard most merchant ships to select and track

their targets. Other factors that contribute to ship vulnerability include substandard vessel maintenance and management, reduced crew size, and lay-ups in high-risk anchorages (Bateman 2010).

Although commercial vessels are generally the focus of modern maritime piracy, cruising yachts have also been captured. In 2011, the 58-ft sailing vessel *Quest* was taken by pirates off the coast of Somalia. Ultimately, in spite of intervention by US Navy Special Forces, the four Americans who made up *Quest's* crew were killed by their captors (Nagourney and Gettleman 2011).

Objectives and Motives

The goals and underlying incentives for modern maritime piracy are largely financial in nature. Although this is a matter of some debate, there is little evidence of political motivation and, in particular, terroristic involvement in current piracy endeavors.

Armed Robbery

Acts of this type are common in Southeast Asia, among other locations. In areas such as those along the coast of the Indian subcontinent, attacks are characterized by the boarding of ships to steal cash, valuables, and in some cases items of cargo. A typical example of this kind of incident is summarized here:

> 05.05.2014: 2155 LT: Posn: 22:08N – 091:46E, Chittagong Roads, Bangladesh.
>
> 30 robbers in a boat armed with long knives approached an anchored chemical tanker. Four robbers boarded the tanker and cut off the aft mooring rope. Alarm raised, crew mustered in the accommodation and Coast Guard informed. Upon hearing the alarm, the robbers stole a lifebuoy and escaped. A patrol boat came to the location and made a search.
>
> (IMB 2014a)

Hijacking and Ransom

Somali piracy is focused on the hijacking of ships and the securing of ransom for their release. An example typical of this type of pirate attack involved the Bahamian-flagged *MV CEC Future*, which was hijacked in November 2008. The pirates were armed with AK-47s, a rocket-propelled grenade launcher, and handguns when they attacked and seized the vessel, which was owned by Clipper Group, a Danish company. The pirates forced the crew to anchor off the Somalia coast and held the vessel, cargo, and 13 crew members captive for 71 days until the owners delivered $1.7 million in ransom to the pirates. One of the two leaders of the pirate group was shot dead in a battle over the ransom as soon as he arrived ashore (Walker 2009).

Ship and Cargo Theft

In some cases, vessels have been hijacked with the intent to sell them or to rename them and use them for illicit purposes or for legitimate service under an illegal owner. In 1998, the Hong Kong-flagged bulk carrier *Cheung Son* was boarded off Taiwan by what appeared to be Chinese customs officers. After boarding the ship, the armed and uniformed pirates held the crew hostage for 10 days, after which all 23 Chinese crew members were beaten to death and thrown over the side. The hijackers then sold the ship to a Chinese buyer for a reported $36,000 (Liss 2003).

In other cases, acquisition of the cargo is the principal focus of maritime criminals. In the span of a single week during April 2014, pirates hijacked two product tankers off Malaysia and stole part of their cargo, in the first instance transferring approximately three million liters of diesel fuel to other vessels. Cargo theft is often the motive for piracy in the Gulf of Guinea.

Methods of Operation

A typical Somali pirate attack involves small, fast, outboard-powered skiffs (often two), which approach merchant ships from dead astern (directly behind the vessel) or on each quarter. An approach from dead astern takes advantage of the radar blind spot in that sector that is typical of the equipment installation aboard many ships.

The skiffs ordinarily approach the ship's side or stern, at which time ladders or grappling hooks are put up over the rail. If this is successful, the pirates are then able to board the vessel. If the ship is steaming too fast for the pirates to achieve their goal of coming alongside and boarding over the rail, they may fire on the ship with automatic weapons such as AK-47s or rocket-propelled grenade (RPG) launchers in an attempt to get the vessel to slow or stop.

Once on board the ship, the pirates typically proceed to the bridge, where they take control of the vessel and her navigation by intimidation of the officers and crew at gunpoint. Off the Horn of Africa, ships that have been thus hijacked are routinely forced to steam into coastal waters, where they are anchored, and negotiations for ransom and the release of the crew, ship, and cargo commence.

While in years past most maritime piracy took place within fairly close proximity to the coastline, pirates in the Western Indian Ocean have evolved a system that employs pirate support vessels, or "mother ships," which are often captured fishing dhows, tugs, or cargo ships that can maintain station far offshore for long periods of time. These mother ships often tow pirate skiffs astern or carry them on deck. Through this tactic, pirates are able to attack ships 1,500 or more miles at sea. This development has introduced very significant challenges for naval patrol and intervention efforts in this region.

Supply Chain Impacts and Costs

Taking a macro view of the situation, it has been estimated that the total annual monetary cost of piracy to the international community is somewhere between $4.9 and $8.3 billion (Geopolicity 2011). Costs and impacts that derive from modern maritime piracy can be grouped into those borne by supply chain partners such as shippers, vessel personnel, and insurers and those that are the responsibility of nations, intergovernmental organizations, military entities, etc. This section discusses the former category.

Mariner Welfare

The effects of hijackings and hostage-takings on vessel personnel are too often overlooked in policy deliberations and analyses of the implications of modern piracy. The crews of merchant ships taken by pirates often endure long, miserable months in captivity, during which time they suffer physical deprivation and psychological trauma. In 2012, there were 349 mariners taken hostage and held by Somali pirates for an average of 11 months; 206 seafarers were captured by West African pirates and held for a mean interval of 4 days (Hurlburt 2013).

The level of violence directed against crew members varies by region and over time. Somali pirates in 2012 reportedly subjected 100 % of their hostages to repeated threats of violence, psychological abuse, and confinement. Fifty percent of Somali pirate hostages experienced direct physical abuse by their captors, and 15 % suffered extreme physical abuse that is best characterized as torture, such as being tied up in the sun for hours, locked in freezers, and having their fingernails pulled out with pliers (Hurlburt 2013). Between 2009 and 2013, 197 seafarers were reportedly injured as a result of maritime piracy worldwide; 33 mariners were killed during the same interval (IMB 2014b).

Crew Compensation

For seafarers aboard ships that transit high-risk areas, hazard pay is often available as a result of agreements with organizations such as the International Transport Federation (ITF) or the national administrations of countries that register ships or provide their crews. In addition, if a ship is hijacked, crew members are often entitled to captivity pay.

The entry into force in 2013 of the International Labour Organization (ILO) Maritime Labour Convention, 2006 (MLC 2006), helped to reinforce the rights of mariners to hazard pay and compensation for periods of captivity. Under the MLC 2006, every seafarer has the right to a safe and secure workplace that complies with

safety standards; fair terms of employment; decent working and living conditions on board the ship; and health protection, medical care, welfare measures, and other forms of social protection (ILO 2013).

One estimate for the total cost of hazard pay and captivity pay for mariners in the Gulf of Aden/ Horn of Africa high-risk area in 2013 is $462.1 million. Seafarers in the Gulf of Guinea high-risk area were paid an estimated $9.2 million in premium compensation (Madsen et al. 2014).

Ransom Payments

Where piracy off the Horn of Africa is concerned, one estimate suggests that in 2011, 31 separate ransoms were paid for the release of ships, crews, and cargoes, amounting to a total of $159.62 million with an average ransom of $4.97 million (Bowden and Basnet 2012). Eight ransoms totaling approximately $32 million were paid to Somali pirates in 2012. The average ransom paid in 2012 was estimated at $3.96 million (Bellish 2013). By the end of 2013, ransoms paid to Somali pirates had further declined to an estimated total of $21.6 million, which amount consists of only three ransoms at an average cost of $7.2 million (Madsen et al. 2014). Costs such as ransom delivery, negotiator and attorney fees, vessel damage, and other items associated with ransom payments may double the cost of ransoms.

While military invention has, in some cases, resulted in the interruption of attacks in progress and the dramatic rescue of hostages from ships that have been hijacked and held for ransom, the challenges inherent in positioning military assets to accomplish these feats are daunting. Figure 1 depicts military personnel training for such missions.

Insurance

There are four basic types of ocean marine insurance (King 2008):

- Hull and machinery (H&M) insurance that covers physical risk to the ship, like grounding or damage from heavy seas, collision, sinking, capsizing, being stranded, fire, piracy, and jettisoning cargo to save other property.
- Cargo insurance that covers the goods transported in the ship.
- Hull war risk insurance (including automatic termination and cancellation provisions in the event of war).
- Protection and indemnity (P&I) which covers liability involving the crew, docks, and piers. Ship owners can purchase separate kidnap and ransom (K&R) insurance for crew members.

The terms of marine insurance policies vary depending on the insurer and the specific conditions of the vessel, the voyage, and perceived and declared risks.

Fig. 1 Commandos engage in an antipiracy exercise aboard the US Merchant Marine Academy Training Vessel *Kings Pointer* (Source: Jon S. Helmick)

Many insurers have delineated the geographic zones in which there is a higher risk of piracy as "war risk" or "additional premium" areas. This designation means that the owners or operators of vessels transiting these waters must pay a surcharge and must also usually notify the underwriter before entering the high-risk zone.

While most ships will be covered for the risk of piracy under either hull and machinery marine risks or war risks policies, K&R coverage will generally be the source of ransom payments. The premiums charged for this coverage depend on such factors as the route and date of the voyage (for individual voyages) or the anticipated number of voyages through high-risk waters (for annual coverage); the name, speed, size, type, and freeboard of the ship; the cargo to be carried; crew particulars; and details of the security measures in place. Reductions in premiums of up to 25 % for a four-man unarmed embarked security team, or up to 50 % if the security team is armed, are possible (Marsh 2011).

The estimated cost of war risk insurance against Somali piracy has dropped by 69 % or $252.2 million from 2012 levels to a total estimated cost of $113.3 million in 2013. The estimated total cost of K&R insurance to protect against Somali pirates was $72,416,124 for 2013, representing a 66 % decrease, or $144,568,547 relative to 2012. These two cost components, taken together, total $185,703,266. The total cost of war risk insurance for West Africa in 2013 was estimated to be $25.2 million, while the total cost of K&R insurance in this area was estimated $14.9 million. Piracy-related insurance premiums in West Africa in 2013 thus totaled an estimated $40 million (Madsen et al. 2014).

Fast Steaming

The surge in Somali piracy coincided with a steep decline in the global economy and very difficult market conditions for the shipping industry. Because fuel is one of the largest operating costs for merchant vessels, in many cases amounting to 25 % of the total, many carriers adopted a strategy of "super-slow-steaming" to minimize fuel consumption. While a given ship might have a top speed of over 20 knots (one knot = 1.15 nautical miles per hour), that same ship might operate most economically at a speed of 12–13 knots (Hooper 2012).

Ships underway are less likely to be targeted and boarded by pirates as their speed increases. The collective recommendations of several industry associations suggest that, thus far, there have been no reported attacks in which pirates boarded a ship that has been steaming at over 18 knots. The recommendations advise ships to proceed at full sea speed, or at least 18 knots if they are capable of greater speed, for the duration of their transit of the high-risk area (this refers to the Gulf of Aden/Horn of Africa region) (BMP4 2011).

The additional fuel costs associated with such "fast steaming" are very significant for carriers. One analysis suggests that vessel owners and operators spent $1.53 billion on increased speeds in 2012. To put this in perspective, it is estimated that one very large crude carrier (VLCC) steaming at 17.9 knots (5.1 knots above the ideal speed of 12.8 knots) incurs $88,681.74 in additional costs per day (Bellish 2013).

Delayed Cargo

Considering the case of Somali piracy alone, it has been noted that trade valued at approximately $463 billion transits the high-risk area off the Horn of Africa each year. If pirate attacks disrupt 2 % of the traffic that passes through the Suez Canal, some $7.4 billion worth of cargo is affected. This is more than the individual GDPs of 75 economies worldwide, including those of Montenegro, Aruba, Liechtenstein, and Somalia (Sullivan 2010).

Piracy interrupts or delays the flow of cargo along the trade lanes where it is a problem. If a ship is hijacked and held for any period of time, the owner or charterer may have to deal with lost revenue and higher charter expenses. Cargo that is delivered late may lose value, if it can be delivered at all. Perishables and commodities such as crude oil—the value of which fluctuates on a daily basis—are particularly problematic. Cargoes in the high-value, time-sensitive sector, such as repair parts, pharmaceuticals, and luxury cars, incur especially substantial additional in-transit inventory carrying costs for their owners.

To address such losses derived from piracy-related delays, some London insurance brokers have created specialized products. Aon developed a policy designed to cover the "financial impact of business interruption or loss of earnings" incurred by charterers, ship owners, and cargo owners. This coverage is triggered from the beginning of a pirate attack, has no deductible, and is a standalone policy intended to complement existing hull, war, cargo, and P&I policies (Siemens et al. n.d.).

Security Equipment and Personnel

Lethal and nonlethal items of security equipment and systems are available to be deployed against pirates.

Equipment that can aid in detection of pirate attacks includes human lookouts, radar, closed-circuit TV (CCTV), search lights, and deck lighting. Physical barriers that can prevent or delay boarding by pirates include razor wire, barbed wire, electric fencing, slippery foam, fire hoses, and water cannons. Examples of crew protective measures include Kevlar jackets, helmets, security glass, and the "citadel," a retreat on board the vessel into which the crew can proceed in the event of an attack and which is ideally stocked with food, water, communications equipment, and, in some cases, means to control the ship.

Defensive equipment includes such devices as the Long Range Acoustic Device (LRAD), which is a hailing device that can emit a pain-inducing tone that is unbearable for the recipient, even at distances of 100 m or more. The LRAD became well-known in the industry in 2005 when the cruise ship Seabourn Pride used one to help repel pirates attempting to board the ship off the coast of Somalia.

The use of firearms by vessel personnel is a hotly debated topic. The IMO and many flag states have strongly opposed the carriage of lethal weapons by ship's crews, arguing that merchant mariners generally lack the training necessary to effectively deploy firearms to repel pirate attacks and that the presence of such weapons may escalate conflicts in a boarding situation, leading to injury or fatalities.

The practice of placing security teams aboard vessels transiting high-risk waters has become increasingly common. The use of qualified and properly managed privately contracted armed security personnel (PCASP) has proven to be generally highly effective in deterring pirate attacks. Ordinarily comprised of former military or ex-law enforcement personnel, embarked security teams typically board the ship prior to the beginning of the passage through areas of pirate activity, disembarking at the first port of call after the high-risk transit. In recognition of the fact that the commercial providers of armed security teams vary widely in the extent to which they vet their personnel and ensure that they are properly trained, the IMO has issued guidance on many of the key issues associated with the use of such teams. Concerns addressed include such matters as command and control, firearms management, applicable law, use of force, insurance, and related matters (IMO 2012). There are also complex questions of liability and weapon carriage associated with the use of embarked security teams.

Efforts to establish professional standards for maritime security teams and the companies that provide them have been undertaken by BIMCO and the Security Association for the Maritime Industry (SAMI). These association-based certification programs provide ocean carriers and shipmasters with some degree of assurance regarding the competence, background, and reliability of the security providers they choose to retain (Yanchunas 2014).

In 2013, expenditures for shipboard antipiracy equipment were estimated to be $247–299 million. Expenses associated with the use of privately contracted armed security personnel amounted to an estimated $767–876 million. Adding in costs of PCASP accreditation and certification, total costs for security equipment and armed guards in 2013 totaled an estimated $1.02–1.18 billion (Madsen et al. 2014).

Risk Management and Resiliency Strategies

Best Management Practices

The *Best Management Practices for Protection Against Somalia Based Piracy* (*BMP4*) is a guide developed by a number of global maritime industry organizations as a means to address the problem of piracy involving merchant ships in the Indian Ocean off the Horn of Africa. The purpose of the BMP—now in its fourth iteration—is to provide specific recommendations on strategies and tactics that can be used to avoid, deter, or delay piracy attacks in the geographic region of concern. The document describes pirate activity, discusses risk assessment, provides guidance on appropriate planning, identifies self-protection measures, delineates possible responses in the event of a pending or actual attack, defines correct action in the case of military intervention, and surveys post-incident reporting practices.

To help address the situation in the Gulf of Guinea, *Interim Guidelines for Owners*, *Operators and Masters for Protection against Piracy* have been developed by BIMCO, ICS, INTERCARGO, and INTERTANKO. These guidelines, which are based on the BMP4, are supported by NATO Shipping Centre (Bimco et al. 2012).

Training, Drills, and Exercises

Appropriate training of vessel personnel in antipiracy tactics and contingency responses is crucially important in the effort to contain and mitigate the threat of maritime piracy.

International requirements for the maritime security training of merchant mariners are delineated in the International Ship and Port Facility (ISPS) Code, which was concluded by the International Maritime Organization (IMO) in London in December 2002. The Code is a "comprehensive set of measures to enhance the security of ships and port facilities, developed in response to the perceived threats to ships and port facilities in the wake of the 9/11 attacks in the United States" (International Maritime Organization). Where antipiracy matters are concerned, the ISPS Code addresses the threat generically, stating the requirements for training of vessel security personnel under such headings as "Recognition of characteristics and behavioral patterns of persons who are likely to threaten security," "Knowledge of current security threats and patterns," "Techniques used to circumvent security measures," and the like. The ISPS Code entered into force on 1 July 2004.

The International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW), 1978, as amended, was established by IMO member nations as a global framework for the development and enhancement of merchant mariner competence. The 2010 Amendments ("Manila Amendments") to the IMO STCW Convention and Code included new requirements for antipiracy training.

The Manila Amendments were the result of a comprehensive review of STCW that was begun in 2006 by the IMO Standards of Training and Watchkeeping (STW) Subcommittee and culminated in a June 2010 Diplomatic Conference in Manila. The Manila Amendments entered into force on 1 January 2012.

The IMO publishes a series of "model courses" that set forth the learning objectives and content for the training of vessel personnel in maritime security and antipiracy subjects. In early 2011, on behalf of the United States, the US Merchant Marine Academy reviewed the mandates contained in the 2010 Manila Amendments and revised the IMO maritime security curriculum to provide (among other enhancements) increased antipiracy competences for merchant vessel personnel worldwide. Of the five courses involved, those that are focused on vessel personnel and that address piracy topics include (1) Ship Security Officer, (2) Security Training for Seafarers with Designated Security Duties, and (3) Security Awareness Training for All Seafarers. The training of merchant marine officers in antipiracy strategies and tactics may also be conducted as part of Bridge Resource Management training, as depicted in Fig. 2.

Of critical importance in the detection, deterrence, and mitigation of piracy and armed robbery are regular drills and exercises aboard ship. The scope and frequency of security drills and exercises are specified in IMO conventions and national laws. A well-planned and thoroughly practiced response to the contingency of an attempted boarding by pirates or robbers can be highly effective in preventing a successful attack or at least minimizing its negative consequences.

Fig. 2 Route planning, evasive maneuvers, and contingency planning are important elements of antipiracy training that can be included in Bridge Resource Management training for merchant marine officers (Source: US Merchant Marine Academy)

Military Intervention

Recognizing the increasing threat to strategically and commercially important global supply chains, ocean carriers, and their personnel, the international community began to deploy naval assets to deter pirates and protect merchant shipping in the Gulf of Aden/Horn of Africa high-risk area.

UN Security Council Resolutions 1814, 1816, 1838, 1846, 1851, and 1897 permit and actively encourage international naval forces to "enter the territorial waters of Somalia" (1816) and to operate ashore "in Somalia for the purpose of suppressing acts of piracy and armed robbery at sea" (1851). Counter-piracy naval operations in the Gulf of Aden/Horn of Africa region include the multinational "Combined Task Force 151 (CTF-151)" led by the United States, "Operation Atalanta" spearheaded by the European Union Naval Force (EUNAVFOR), and "Operation Ocean Shield" under NATO. At various times, a number of countries including China, Japan, Iran, India, and Russia have deployed naval vessels in the area to fight piracy outside the framework of these missions. An estimated 40 naval vessels are typically engaged in counter-piracy missions in the Western Indian Ocean, Gulf of Aden, and off the Horn of Africa (Stockbruegger 2010).

A major problem with the naval solution to piracy is the vastness of the ocean in which pirates operate. As a matter of practicality, there is simply no way to position naval vessels in close enough proximity to all of the merchant ships passing through the Gulf of Aden/Horn of Africa/Western Indian Ocean to provide effective deterrence or the possibility of rescue.

Corridors and Group Transits

As a means of enhancing security for vessels transiting waters at high risk for piracy in the Gulf of Aden, an Internationally Recommended Transit Corridor (IRTC) has been established. The corridor is 492 miles long and has an eastbound lane and a westbound lane. Each lane is 5 miles wide with a 2-mile separation zone between the lanes. Warships are strategically deployed in and around the IRTC to deter attacks and provide support if vessels are approached or boarded. The IMO provides guidance on procedures and protocols for use of the IRTC through SN.1/Circ.28 "Information on Internationally Recommended Transit Corridor (IRTC) for Ships Transiting the Gulf of Aden" (IMO 2009). The location and configuration of the IRTC are shown in Fig. 3.

Merchant ships are encouraged to transit the IRTC in groups. The timing of these group transits is defined by the Maritime Security Center Horn of Africa (MSCHOA) operated by EUNAVFOR. The key objectives are to group vessels according to their speed, time their transit through the highest-risk areas to avoid hours of peak attack incidence, and position vulnerable merchant ships so that they can be best protected by available naval assets.

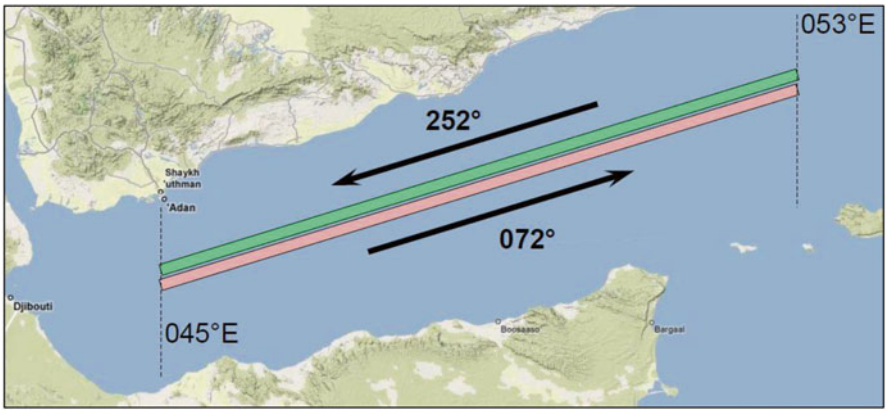


Fig. 3 Internationally Recommended Transit Corridor, Gulf of Aden (Source: NATO Shipping Centre)

Rerouting and Supply Chain Reconfiguration

A seemingly obvious means of dealing with the threat of piracy and armed robbery is avoidance of the trade lanes and port zones where it is known to occur. Rerouting of ships to avoid piracy-prone areas is one option, but one that often involves considerable complexity in the calculation of cost-benefit ratios.

Deviation from established shipping lanes generally involves longer voyages and higher crew costs, fuel costs, other operating costs, and in-transit inventory costs. Rerouting may make the most sense for ships carrying lower value, bulk cargoes. However, for high-value consumer goods or items needed for just-in-time manufacturing, the added delay may be unacceptable to the shipper. In addition, such cargoes are usually carried in container ships capable of higher speeds, which are less likely to be attacked while underway than tankers and bulk carriers.

As an example, rerouting a tanker from Saudi Arabia to the United States around the Cape of Good Hope instead of through the Suez Canal and Gulf of Aden adds approximately 2,700 miles to the voyage. This longer distance reduces the number of voyages the ship can make in a year (from about six to five—a drop of 26 %). This, in turn, reduces the capacity of the particular supply chain of which that vessel is a part. Routing via the Cape of Good Hope in this example incurs additional costs of about $3.5 million annually (MARAD 2010).

With the dramatic decline in piracy in the Gulf of Aden/Horn of Africa region, available evidence suggests that significant route deviation is no longer taking place. Costs associated with vessel rerouting to avoid piracy are estimated at $0 for 2013, down from $290.5 million in 2012 (Madsen et al. 2014).

Avoidance of particular ports and harbors where armed robbery is problematic is typically not a feasible option. Ships, especially tankers and bulk carriers, are dependent in most cases on specific infrastructure and cargo locations for which alternatives are not readily available.

A more permanent and radical approach to the problem of maritime piracy is shifting production or processing to a location that reduces or eliminates exposure to piracy-prone areas. For example, relocation from China to Mexico of a manufacturing plant for electronic devices destined for the Canadian market essentially eliminates the risk of piracy. The difficulties with this type of "nearshoring" strategy include the facts that it may be very expensive to implement and that for many commodities such as petroleum, the site of production is fixed. In addition, areas that are at high risk for piracy and armed robbery may shift over time, possibly obviating the enhanced security achieved by supply chain reconfiguration.

Conclusion

Andrew J. Shapiro, then-Assistant Secretary of the US State Department Bureau of Political-Military Affairs, summarized the broader ramifications of Somali piracy as follows (2011, 30 Mar):

> …the modern day implications of piracy are now global in scope. In today's globalized age the problem of piracy is one that affects not just individual countries or shipping companies but potentially the entire global economy. We live in an era of complex and integrated global supply chains where people in countries around the world depend on safe and reliable shipping lanes for their goods, their energy, their medicine, and basic consumer goods. By threatening one of the world's busiest shipping lanes, piracy off the Horn of Africa threatens not just specific ships, but has broader strategic implications.

This statement underscores the critical importance of refusing to allow the criminal opportunists that are modern-day pirates to impede the flow of global commerce. In addition, protection of the world's seafarers from the scourge of maritime piracy must be considered a top priority.

For the moment, it appears that the threat of Somali piracy has been largely contained. The debate will no doubt rage over which factors are responsible for this success, but some combination of the deployment of embarked security teams, the application of Best Management Practices, and combined naval patrols and intervention is likely responsible.

Piracy and armed robbery in other parts of the world continue unabated and, in some locations such as the Gulf of Guinea, are increasing in frequency. Some of the same countermeasures that have been employed in the fight against Somali piracy may have application elsewhere, but there are limitations. For example, the use of PCASP is prohibited in the territorial waters of Nigeria, Togo, and Benin, where guards must be obtained from local military forces (International Group 2013).

Ultimately, the solution to piracy may involve shoreside law enforcement capacity building, enhanced governmental stability, and the development of viable and attractive economic alternatives for those who engage in piracy. Failing this kind of evolution, the maritime industry and affected national administrations will be obligated to continue to work toward the creation of effective short-term strategies and tactics to detect, deter, and defend against maritime piracy.

References

Banerji A, Jose D (2013) Murder trial of Italian marines in India navigates murky waters. Reuters. http://in.reuters.com/article/2013/06/10/india-italy-marines-idINDEE95900B20130610. Accessed 1 May 2014

Bateman S (2010) Maritime piracy in the Indo-Pacific region—ship vulnerability issues. Marit Policy Manag 37(7):737–751

Bellish J (2013) The economic cost of Somali piracy 2012. Oceans Beyond Piracy. http://oceans-beyondpiracy.org/sites/default/files/attachments/View%20Full%20Report_1.pdf. Accessed 4 Feb 2014

BIMCO et al (2012) Interim Guidelines for Owners, Operators and Masters for protection against piracy in the Gulf of Guinea region. https://www.bimco.org/~/media/Security/Piracy/Gulf_of_Guinea/2012-12-20_RT_agreed_GoG_anti-piracy_guidance.ashx. Accessed 13 Mar 2014

BMP4 (2011) Best management practices for protection against Somalia based piracy. Witherby, Edinburgh

Bowden A, Basnet S (2012) The economic cost of Somali piracy 2011. Oceans Beyond Piracy. http://oceansbeyondpiracy.org/sites/default/files/economic_cost_of_piracy_2011.pdf. Accessed 6 Feb 2014

Geopolicity (2011) The economics of piracy. http://www.geopolicity.com/upload/content/pub_1305229189_regular.pdf. Accessed 14 May 2014

Hooper E (2012) The shipping industry and the spiraling costs of maritime piracy. http://www.counterpiracy.ae/upload/Briefing/Eirik%20Hooper-Essay-Eng-2.pdf. Accessed 7 May 2014

Hurlburt K (2013) The human cost of maritime piracy 2012. Oceans Beyond Piracy. http://oceans-beyondpiracy.org/sites/default/files/attachments/View%20Full%20Report.pdf. Accessed 7 Feb 2014

International Group (2013) Piracy—FAQs. http://www.ukpandi.com/fileadmin/uploads/uk-pi/Documents/Piracy/Piracy_FAQs_RevisedAug2013_web.pdf. Accessed 6 May 2014

International Labour Organization (ILO) (2013) Basic facts on the Maritime Labour Convention 2006. http://www.ilo.org/global/standards/maritime-labour-convention/what-it-does/WCMS_219665/lan--n/index.htm. Accessed 14 Apr 2014

International Maritime Bureau (IMB) (2014a) Live piracy & armed robbery report 2014. http://www.icc-ccs.org/piracy-reporting-centre/live-piracy-report. Accessed 24 May 2014

International Maritime Bureau (IMB) (2014b) Piracy & armed robbery against ships—2013 annual report

International Maritime Organization (IMO) (2009) SN.1/Circ.281. Information on Internationally Recommended Transit Corridor (IRTC) for ships transiting the Gulf of Aden. http://www.imo.org/OurWork/Security/PiracyArmedRobbery/Guidance/Documents/SN.1-Circ.281.pdf. Accessed 21 May 2014

International Maritime Organization (IMO) (2011) Circular letter No. 3180. Circular letter concerning information and guidance on elements of international law relating to piracy. http://www.un.org/depts/los/piracy/circular_letter_3180.pdf. Accessed 12 Jan 2014

International Maritime Organization (IMO) (2012) MSC.1/Circ.1443. Interim guidance to private maritime security companies providing privately contracted armed security personnel on board ships in the high risk area. http://www.imo.org/OurWork/Security/SecDocs/Documents/Piracy/MSC.1-Circ.1443.pdf. Accessed 22 May 2014

King RO (2008) Ocean piracy and its impact on insurance. Congressional Research Service. http://fpc.state.gov/documents/organization/115925.pdf. Accessed 14 May 2014

Liss C (2003) Maritime piracy in Southeast Asia. Southeast Asian Aff 2003:52–68

MAREX (2014) 70 pirate attacks in 2014 so far–Dryad. The Maritime Executive. http://www.maritime-executive.com/article/70-Pirate-Attacks-in-2014-So-Fa--ryad-2014-04-09/. Accessed 9 Apr 2014

Madsen JV et al (2014) The state of maritime piracy 2013. Oceans Beyond Piracy. http://oceans-beyondpiracy.org/sites/default/files/attachments/SoP2013-Digital_0.pdf. Accessed 6 May 2014

Maritime Administration (MARAD) (2010) Economic impact of piracy in the Gulf of Aden on global trade. http://www.marad.dot.gov/documents/Economic_Impact_of_Piracy_2010.pdf. Accessed 27 May 2014

Marsh (2011) Piracy--The insurance implications. http://www.igpandi.org/downloadables/piracy/news/Marsh%20Piracy%20implications.pdf. Accessed 12 May 2014

Nagourney A, Gettleman J (2011) Pirates brutally end yachting dream. New York Times. http://www.nytimes.com/2011/02/23/world/africa/23pirates.html?pagewanted=all&_r=0. Accessed 22 Feb 2014

NATO Shipping Centre. http://www.shipping.nato.int/operations/OS/Pages/GroupTransit.aspx. Accessed 15 May 2014

Shapiro A (2011) Approaches to counter-piracy. Remarks to International Institute for Strategic Studies. http://m.state.gov/md159419.htm. Accessed 3 Apr 2014

Siemens RL et al (n.d.) Piracy's impact on insurance. Risk Management Magazine. http://cf.rims.org/Magazine/PrintTemplate.cfm?AID=3959. Accessed 20 May 2014

Stockbruegger J (2010) Somali piracy and the international response: trends in 2009 and prospects for 2010. Piracy Studies: Research Portal for Maritime Security. http://piracy-studies.org/2010/somali-piracy-and-the-international-response-trends-in-2009-and-prospects-for-2010/. Accessed 28 May 2014

Sullivan AK (2010) Piracy in the Horn of Africa and its effects on the global supply chain. J Transp Secur 3:231–243. doi:10.1007/s12198-010-0049-9

Walker R (2009) Inside story of a Somali pirate attack. BBC News. http://news.bbc.co.uk/2/hi/8080098.stm. Accessed 16 Apr 2014

Yanchunas D (2014) Masters, shipowners face liability risk from armed guards' mistakes. Prof Mariner :41–44

Political Risk to the Supply Chain

Terrorist and Criminal Groups and State Posing a Threat to the Global Supply Chain: An Overview

John Harrison

Abstract The chapter offers three key points: an examination of how terrorist and criminal organisational structures have a direct impact on the threat posed to the global supply chain, a global and regional overview of the terrorist and criminal threat to the supply chain in each region and, third, some general approaches to responding to varying threats. The global and regional overview of the security threats faced by maritime, civil aviation and rail transportation. The chapter discusses the importance of understanding how terrorist and criminal groups organise and how that impacts their capabilities and opportunities to interfere with the supply chain. There is an understandable focus on the global threat here from al-Qaeda and its various affiliates and offshoots; the key concerns are the metalising regional threats and their potential global impact. The chapter argues that the diversity of threats faced require an equally diverse range of responses utilising both traditional approaches and deploying intellectual tools that have to date been underutilised.

Keywords AQC • AQAP • ISIL • D Company • Cartels • Civil aviation • Maritime • Rail • Middle East • Southeast Asia • East Asia • Central Asia • South Asia • Europe • Africa • South America • North America • Piracy • Al-Shabaab

---

Disclaimer: The views expressed here are those of the author and do not represent the official positions of Cyberpoint LLC or its clients.

This chapter focuses on non-state actors and their threats to the global supply chain. The main reason is that non-state actors are more likely than states to interfere with the supply as states have economic incentives to maintain the supply chain that non-state actors do not. Additionally, the chapter will focus primarily on aviation; even though it is the smallest component of the global supply chain, it is the primary target for non-state actors.

J. Harrison (✉)
Cyberpoint International LLC, Dubai, UAE
e-mail: Johnjharrisonnsc@yahoo.com

A.R. Thomas, S. Vaduva (eds.), *Global Supply Chain Security*,
DOI 10.1007/978-1-4939-2178-2_3

Introduction

In the past decade, the focus of supply chain security has been on countering the terrorist threat. While terrorism certainly is a real and immediate concern, with perpetrators constantly trying to stay one step ahead of the industry's latest measures, threats from other corners must not be overlooked. Criminals use the supply chain as a conduit for the trafficking of contraband and people, and theft is a constant concern across the supply chain. Furthermore, criminal gangs have been found to be operating ports and airside at airports around the world. The largest single threat to the supply chain however arises from state interference with its operations. This chapter outlines all the current threats facing the global supply chain, from an up-to-date overview of the terrorist threat pertinent criminal issues and potential state disruptions. This chapter will begin with the global terrorism threat and then turn to the organised criminal threats.

The last decade has been dominated by an ongoing series of assertions primarily focusing on the changing nature of organisations. The highly interconnected world, the main argument offers, no longer requires hierarchical organisations. In fact, the speed required to function in a 24/7 world requires a flatter, decentralised network structure to adequately adapt to the rapidly changing world. Gone are the days where a CEO, a mafia don or a terrorist leader can or should dictate operational details. These leaders exist, but their role is now reduced to merely establishing strategic direction and perhaps selecting the correct senior staff to assist in implementation. It is in the terrorist and criminal world where this has been most clearly demonstrated.

The second assertion, which has increasing empirical support, is the critical role social movements play in forming social awareness and protest, which frequently embraces violence as a critical means of addressing social grievances. The critical levels of analysis for social movement theory are grievance identification, resource mobilisation, the role of violence and organising for violence. A more comprehensive discussion of this useful theory is beyond the scope of this chapter, but it is important for industry professionals to have a general understanding of the wider context and roots of what they face in order to develop a defence in depth to current and future threats.

This work defines political risk as the use or disruption of the civilian supply chain due to the actions of terrorist or criminal actors. While the supply chain is overwhelming maritime and land transportation focused (rail and truck) the terrorist and in many cases criminal groups focus on international civil aviation, thus this chapter will share that focus.

What Next for Al-Qaeda?

Three years after the death of Osama bin Laden, al-Qaeda (AQ) core has been unsuccessfully attempting to reassert itself as an organisation. Operationally, AQ core has been significantly degraded. Ayman al-Zawahiri has become the head of

the AQ core, but as the struggle with the former AQ affiliate the Islamic State of Iraq and the Levant demonstrates, he has yet to establish his operational bona fides. This may be part of a larger strategy of shifting the core from an operational to an inspirational role, or it may suggest al-Zawahiri's inability to assert his authority. The 'conference call' indicating an imminent attack (intercepted by the United States) that caused disruption to and closure of diplomatic operations for many Western nations in August of 2013,[1] along with media reports that have thus far emerged from the intelligence recovered from Abbottabad, suggests that bin Laden was much more involved in operational details than previously understood. It seems logical that al-Zawahiri will attempt to replicate the effort. Irrespective of who the titular head of AQ is, the organisation has been attempting to reassert itself both from the AQ core in tribal areas of Pakistan and with its name-brand affiliates, the most prominent being al-Qaeda in the Arab Peninsula (AQAP). AQ has been struggling for relevancy for much of the last several years, and events in the Arab Spring of 2011 have only accelerated the need to regain its position as setting the agenda for the Arab and Islamic world. It is currently assumed that from the AQ core perspective, it matters little which franchise drives the agenda, only that AQ's name is attached. The analytical assumptions driving this remain speculative and are most likely changing with what is assumed to be a power struggle within AQ. It is well beyond the scope of this chapter to engage in speculation over the nature of al-Zawahiri's position as the leader of the AQ core, but it is clear that his attempt to quickly consolidate his position both within AQ and the wider so-called jihadi movement has not been fully successful. Given AQ's commitment to low-frequency but high-consequence attacks and its historic attention to civil aviation, it requires no significant leap to say that the threat environment is increasing dramatically.

Beyond the Pakistan-based core are the affiliated groups: al-Qaeda in the Islamic Maghreb (AQIM), its North African affiliate, Jabhat al Nusra in Syria, al-Qaeda in the Southeast Asian Archipelago (AQSEA) and al-Qaeda in the Arabian Peninsula (AQAP). It is the latter two that have posed the most significant threat to civil aviation and potentially to maritime operations, with AQAP appearing to be the more aggressive in grasping the mantle of leadership within the wider AQ. The most prominent operational figure within AQAP is bomb maker Ibrahim Hassan al-Asiri, who is responsible for the October 2010 cargo bomb plot, using a device hidden in toner cartridges, and the bomb used in the attempt to blow up Northwest flight 253 on Christmas Day 2009. AQ's offshoots and their attacks demonstrate its evolutionary ability as well as its continuing interest in committing terrorist spectaculars targeting international civil aviation.

The weakness of the Yemeni state has traditionally offered AQ a safe haven and laboratory for tactical innovation. It was here in October of 2000 that Abdulrahim Mohammed Abd, AQ's Prince of the Seas, conducted maritime attacks against the

[1] http://www.longwarjournal.org/threat-matrix/archives/2013/08/the_press_quickly_learned_that.php

USS Cole and the October 2002 attack on the MV Limburg.[2] It is unlikely that AQAP, or any of the AQ affiliates, has abandoned its interest in maritime operations, but the inactivity over the last 12 years suggests that its intentions and capabilities are focused elsewhere. It should be remembered that there are many strategic, operational and tactical issues raised by the emergence of AQ's affiliate in the Arabian Peninsula. One issue that has improved is the increasing abilities in intelligence collection and dissemination. The cargo bomb plot was exposed as a result of human penetration of AQAP and the intelligence gained being shared in a timely manner. The evolving nature of the AQAP threat rests on the political changes underway in Yemen and the critical intelligence cooperation demonstrated by the foiling of the 2010 plot. This chapter will highlight key issues in three areas: terrorists' structures and the threat to aviation, ideologies and regions of concern for civil aviation. The critical aim is to predict possible threats before they emerge to perhaps prevent them or, at the very least, develop and deploy responses prior to the emergence of the threat. This breaks the notorious reactive approach to security.

Iran and Hezbollah Prepare for War?

The Lebanese Shia organisation Hezbollah (Party of God) has had a remarkable trajectory. From its founding as a small Shia militia during Lebanon's civil war, it is the largest participant in the governing coalition ruling Lebanon and is a key strategic asset for its patron Iran. The range of charitable, commercial, political, criminal and armed activities it is involved with make it difficult to properly characterise Hezbollah's nature. While engaging in armed struggle, the organisation has undeniably, and intentionally, engaged in prohibited actions which include attacks against civil aviation. The architect of this terrorist campaign was Iyan Mugneigh, who symbolised terrorism during the 1980s until the emergence of Osama bin Laden. The primary concern has been whether Hezbollah would restrict itself to retaliation or strike first against the United States and its interests should Iran's nuclear programme draw military attention. The primary area of operations for Hezbollah is the Middle East, but it should be remembered that they have extensive support networks in Europe, Africa, North America and Asia. It has conducted, or at least allegedly been involved with, operations in Europe, North America (the JFK plot[3]), South America as well as Asia, specifically targeting civil aviation in the Middle East and Latin America. Given the tensions with Iran and Hezbollah's involvement with Syria, the threat from Hezbollah to international civil aviation, and potentially shipping and offshore energy platforms with its acquisition of Chinese made C-802 antiship missiles from Iran[4], is increasing in both nature and scope.

[2] http://www.jamestown.org/single/?no_cache=1&tx_ttnews%5Btt_news%5D=455#.U_BO0lYnKDU

[3] http://www.nyc.gov/html/nypd/html/pr/plots_targeting_nyc.shtml accessed June 10, 2013.

[4] Mazzetti and Shanker (2006).

Terrorist Organisations

There are three types of terrorist structures: linked, semi-linked and independent cells. There is also a fourth type, known as lone wolf terrorism, which, by definition, lacks any structure.[5] The perpetrators of the 11 September 2001 attacks may be regarded as members of linked cells. These were full members of AQ and received training, logistical support and significant direction from the central leadership. Due to the extensive training and other support, these cells pose the most significant threat to aviation but are also the most frequently detected by intelligence and security agencies.

Semi-linked cells, such as the 2006 liquid bomb plotters, emerged from the local 'home' environment and had sufficient connections to the wider radical movement to receive at least rudimentary training in the tribal areas of Pakistan. If AQ had any awareness of the cell, it was only shortly before their training, and they had no control over the operation. The lack of training and support makes it harder to detect the cell, but it also reduces their chances of success. They pose a high threat to civil aviation and particularly ground operations.

The 2013 Boston Attack or the 1995 Oklahoma City bombers are examples of an independent cell. While part of the wider so-called jihadi movement, Dzhokhar and Tamerlan Tsarnaev do not appear to be members of a group, and there is little public evidence that either received training from any group.[6] The most notorious attack from an independent cell in the United States was that of Oklahoma City. Neither Timothy McVeigh nor co-conspirators Terry Nichols and Michael and Lori Fortier were part of an organised group. This small signature makes detection almost impossible, albeit their lack of any external support lowers the probability of success. The attack on the Alfred P. Murrah Federal Building in Oklahoma City was a rare success story for cells of this nature. These types pose a limited risk to in-flight aviation but a higher risk to ground infrastructure.

Finally, there are the so-called lone wolves, terrorists who act as individuals. The most famous example is Ted Kaczynski, the Unabomber, who was caught in 1996 after he threatened to attack US civil aviation unless his manifesto was published.[7] While these individuals may be almost impossible to detect, they are less likely to conduct a successful attack of any significant scale and, other than to mass transit, pose a minimal threat to the supply chain.

[5] Harrison (2011), p 22.

[6] http://politicalticker.blogs.cnn.com/2013/04/21/house-homeland-security-chairman-believes-suspect-trained-in-russia

[7] http://www.washingtonpost.com/wp-srv/national/longterm/unabomber/manifesto.text.htm

The Ideological Threats

The key issue to remember is that much terrorism is a sociopolitical act using violence to impose an ideology on a wider population. There are four primary ideological motivations for terrorism: ethno-national, revolutionary/reactionary, religio-political and single issues. Each ideology has dominated a particular historical period, and with the exception of single-issue groups, all have impacted international civil aviation.

Ethno-national terrorism is driven by the desire to have an independent ethnic state (Kurds, Tamils, Palestinians or Basque), leave an existing state to join their co-ethnics across the border (Northern Ireland, Kashmir) or, at least, have wider autonomy (Moros of southern Thailand). It was an ethno-nationalist group, the Marxist-leaning Popular Front for the Liberation of Palestine (PFLP), that, commencing in 1968, introduced attacks against civil aviation as a primary tactic.

Revolutionary/reactionary terrorism is driven by a desire to change the current political orientation of a society either to the left, as in the case of the Red Army Faction (RAF) in Germany, FARC in Colombia and the New People's Army in the Philippines, or to the right, as in the case of the Order Novo in Italy and Aryan Nations in the United States. There are also groups whose aim is to prevent the change that the leftist and rightist groups desire, such as Autodefensas Unidas de Colombia (AUC) in Colombia and the Ulster Defence Association (UDA) in Northern Ireland. The threat to civil aviation has to date come from the left wing groups such as the RAF and FARC.

Religio-political terrorism presents the most pernicious threat today. The primary threat originates from jihadi groups, particularly AQ and its affiliates, but also from Islamist groups such as Hamas, Hezbollah and Lashkar-e-Taiba. The threat is not limited to these groups – there is a rising militant Hindu fundamentalism in India, Jewish fundamentalism in Israel and even Christianity has violent fringe elements. Historically, other religions have targeted aviation. Sikh fundamentalists operating in Canada were held responsible for the Air India flight 182 bombing[8] in 1985, and, in Sri Lanka, Tamil Tigers perpetrated an extensive guerrilla campaign which included the bombing of Air Lanka flight 512 in 1986 and the assault on Bandaranaike Airport in 2001 which wiped out a quarter of Sri Lankan Airlines' Airbus fleet.

Additionally, cults such as the infamous Aum Shinrikyo should not be forgotten. Irrespective of the faith of these movements, they all share a radical interpretation of the faith, a basic binary view of the world and, most critically, a moral obligation to use extreme violence.

Finally, single-issue groups are usually focused on environmental issues (Earth Liberation Front or the Animal Liberation Front) or radical pro-life issues (Army of God). These groups are advocating change in a single issue and are willing to engage in violence. The former poses a potential threat to civil aviation as the

[8] http://www.cbc.ca/news/background/airindia/bombing.html

environmental movement has been increasing their focus on the aviation industry with civil disobedience such as the protest at the Houses of Parliament and Stansted Airport in the UK over the last several years.[9] As these protests have been ineffectual, it is likely that more violent direct action will emerge.

Having briefly discussed the ideologies, we now turn to the global and regional situation, to discuss the current threats faced by the transportation industry.

The Global Situation

The primary threat faced by the supply chain is from the so-called jihadi groups. AQ's ability to replenish and adapt makes it the tier one threat facing civil aviation for the foreseeable future. Its key abilities are to provide its affiliated groups with the wherewithal to escalate from locally focused organisations to ones with global reach and, most critically, the transmission of its ideology through a simple but powerful narrative. This allows for cells and individuals from a wider spectrum of society to become attracted to the call and hence provides a large pool of potential operatives and targets. The key strategic shift in the jihadi movement echoes the environmentalists: think globally but act locally. Thus, we will now highlight the threats emerging in regions around the world.

Groups of Concern Operating in the Middle East

Of the four ideologies mentioned above, only some ethno-nationalist and religio-political conflicts are of concern in this region. In the first instance, ethno-nationalist struggles comprise the Palestinian campaign against Israel and the Kurdish struggle against Turkey. The former struggle is now dominated by religio-political groups like Hamas and will be covered below. The key ethno-nationalist struggle is faced by Turkey.

Kurdistan Workers' Party

The Kurdistan Workers' Party (better known as the PKK) is the primary ethno-nationalist threat group in the region. Despite massive reduction in their capacity, currently numbering 3,000–4,000 from a peak of 90,000, they remain committed to seeking an independent Kurdish state covering parts of Turkey, Iraq, Iran and Syria. The vast Diaspora community in Europe, as well as the financial muscle from heroin trafficking, has permitted the group's survival. Their shift of fighters to Kurdish areas of Syria is a significant escalation in threat to regional security.

[9] Siddique (2008).

Their targeting of the supply chain has been focused in aviation, and that threat remains limited. The PKK conducted a prominent hijacking in 1998, in which a PKK member armed with a pistol and grenade took control of a Turkish Airlines flight before being killed by Turkish counterterrorist forces. The group is also believed to possess anti-aircraft weapons and is suspected of involvement in a 1992 attack in which a Turkish airliner departing the city of Adana was fired upon with automatic weapons. The limited record indicates internal prohibitions against targeting civil aviation, and there is no indication that this has substantially changed.

Al-Qaeda in the Arabian Peninsula

As the attack against Northwest flight 253 and the cargo bomb plot graphically illustrate, al-Qaeda in the Arabian Peninsula (AQAP) has developed into a significant threat to commercial aviation, and given the history of maritime attacks in Yemen, it is surprising that AQAP does not appear to have conducted any operations against maritime assets. The group and its place in the complex situation in Yemen are covered elsewhere. It is sufficient to mention that the group arose from the merger of al-Qaeda's Saudi and Yemeni branches and has received an influx of personnel from al-Qaeda in Pakistan as well as its global network. This helps account for its impressive ability to design and camouflage explosive devices. Like Somalia and Pakistan, Yemen is a common destination for radicalised Westerners seeking training in combat skills, which provides AQAP with its ability to conduct attacks against targets outside the Middle East. The continuing political instability in Yemen makes it very difficult for the state to deploy its limited resources against AQAP, which allows them to more fully exploit their advantageous position in that country. The Yemeni state's inability and AQAP's proven ability to operate beyond its core theatre make it the most threatening group in the al-Qaeda universe.

Hamas and Hezbollah

Each group is battling Israel in an effort to establish an Islamic state in Palestine for Hamas and a Shia-dominated state in Lebanon for Hezbollah. Hamas has to date not conducted an attack against the transportation industry and seems unlikely to do so in the future. Hezbollah, on the other hand, has engaged in hijackings, such as flight TWA 847 in 1985 and Kuwait Airways flight 422 in 1988, and has been linked to maritime attacks in the Red Sea during the mid-1980s. As mentioned above, it has acquired antiship missiles from Iran but has to date only used them against the Israeli Navy. Hezbollah's global network and Iranian control of Hezbollah suggest that if a wider conflict erupts between Iran and other powers, Hezbollah could be unleashed, increasing the threat to the international supply chain.

Iraq

Remnants of al-Qaeda in Mesopotamia (AQM), now called the Islamic State of Iraq and the Levant (ISIL), dominate the Iraqi conflict. They, and other insurgent groups, have access to MANPADS, but their lack of use is interesting. The only successful MANPAD attack against commercial aviation was against a DHL cargo flight departing Baghdad International Airport in 2003. The threat from Iraq is more localised but could be shifting with the growing role of radical sectarian groups for Iraq in the Syrian conflict. Iraq's internal stability remains a question.

Syria

The deteriorating situation in Syria is the largest unknown in the region. What started as a revolution against the Assad regime in March of 2011 has transformed into a wider regional and sectarian conflict involving the Free Syrian Army (FSA) secular 'democrats', local Sunni radicals and regional Sunni radicals, Iran, Hezbollah and Shia radicals from Iraq. A wider war, ensnaring Jordan, Lebanon, Israel and other powers, would have a significant impact on civil aviation. The non-state radicals of both communities would see civil aviation as a way of seeking revenge (for action or inaction in the conflict) as well as political leverage against opponents. As the EU, the United States, Russia and others become entangled in the quagmire, their carriers may pay a steep price.

Groups of Concern Operating in Africa

The primary terrorist threat in Africa (criminal groups are the larger threat and will be covered later below) derives from al-Qaeda and its related groups. The great independence and ideological struggles that defined Africa during the Cold War have given way to ethno-nationalist (tribal) struggles that have had little impact beyond the continent. These groups have posed little threat to the international supply chain. Al-Qaeda has an operational presence in East Africa dating to at least 1998 and has focused primarily on aviation aspects of the supply chain. Its abilities against civil aviation manifested in 2002, when, as part of a coordinated attack against the Paradise Beach Hotel, it attempted to shoot down an Israeli Arkia Airlines flight taking off from Mombasa, using an SA-7 surface-to-air missile. The primary threats in Africa are from al-Shabaab and al-Qaeda in the Islamic Maghreb (AQIM).

There are also some guerrilla groups fighting for regional causes, such as the Movement for the Emancipation of the Niger Delta (MEND), in Nigeria, but they are not thought to be a significant threat to civil aviation.

Al-Shabaab

Al-Shabaab, an Islamist insurgency group operating in southern Somalia, a descendant of the now-defunct Islamic Courts Union, is pursuing an increasingly international agenda and has strong ties with al-Qaeda. The group's attack against Kampala, Uganda's capital, in July 2010, in which 74 people were killed whilst watching a FIFA World Cup match, was the first operation conducted outside Somalia and underscores its increasing regional aspirations. It has been able to recruit fighters from South Asian, Arab and Chechen jihadis in recent years and has successfully recruited young Somali-Americans to commit suicide attacks in Somalia on its behalf. These include an attack against civil aviation using the same method as Northwest flight 253 bomber Umar Farouk Abdulmutallab. In addition, al-Shabaab is thought to be in possession of the SA-18 'Grouse' and other advanced MANPADS. These are allegedly provided by Eritrea,[10] which views conflict in Somalia as an opportunity to fight a proxy war against its rival, Ethiopia. One of these MANPADS may have been deployed against EW 78849 in March 2007 killing all 11 on board.[11] Given the alleged access to weapons, long-term connections to AQ and increasing global orientation, it remains difficult to explain the lack of operational sophistication from al-Shabaab. Thus, while there is potential threat to civil aviation in the Horn of Africa, it remains unactualised.

Al-Qaeda in the Islamic Maghreb

In North Africa, the affiliate group al-Qaeda in the Islamic Maghreb (AQIM) poses a growing threat to international aviation. AQIM emerged from the Algerian Civil War of the 1990s and has absorbed a range of other jihadi groups in the region. AQIM has a highly capable operational capacity, as well as an extensive smuggling and support network in the trans-Sahel region, particularly Mauritania, Mali and Niger. This is augmented by a fundraising and operational network in Spain, France, Italy and elsewhere in Europe. It is also believed to have smuggled fighters to Iraq and has opaque links in Southeast Asia.

AQIM's smuggling networks are thought to be involved in trafficking Latin American cocaine from West Africa to Europe via North African states, which may be shifting the group from an ideological body to a criminal enterprise. Irrespective of the apparent shifting motivations and intense security focus on the region, there is a significant threat to civil aviation in North Africa.

[10] "Report of the Monitoring Group on Somalia," UN Monitoring Group on Somalia, July 18, 2007.

[11] http://aviation-safety.net/database/record.php?id=20070323-0 retrieved June 10, 2013.

AQIM has spanned several smaller groups the most infamous being al-Mulathameen or al-Mua'qi'oon Biddam led by Mokhtar Belmokhtar. Belmokhtar split from AQIM for a variety of reasons[12] and his group dramatically emerged in January 2013 with the mass hostage taking at the Amenas gas facility. The main objective of the operation appears to have been Belmokhtar's effort to establish his operational bona fides and less about the stated demands. His unconfirmed death in March of 2013 may limit the group's immediate impact. The critical point is that the most dramatic terrorist attack in Algeria in years was a function of internal political dynamics within the increasingly fragmented so-called North African jihadi movement. The pressure to gain status through dramatic action creates an increased potential for aviation-related threats.

Boko Haram

Boko Haram has begun to develop a more sophisticated capacity and pose a wider regional threat.[13] The jihadi group emerged in northeastern Nigeria in 2001 and appears to have become more regionally active in the last few years. While it has to date demonstrated little interest in attacking Western interests nor the capability of engaging hard targets, the deteriorating situation in North Africa may rapidly alter this situation. The recent American issue of a reward for the capture of Boko's leadership suggests there is a growing concern for the group.[14] The December 2013 attack on the Maiduguri airbase in northern Nigeria may suggest a shift in the group's tactics.[15] Aviation ground operations should increase vigilance.

There is also a growing concern over the situation in Egypt, especially in the Sinai Peninsula, which is worrying. The militant group Ansar Beit al-Maqdis posted a video apparently showing a helicopter using an SA-7 MANPAD.[16] This is the first confirmed use of a MANPAD in Egypt and presents a significant danger to both military and civil aviation. In July of 2013, the Al Furqan Brigades attacked a container ship transiting the Suez Canal.[17] This was one of a series of attacks and plots against the canal and represents a potential threat to this vital transit point.

---

[12] http://www.policymic.com/articles/45177/al-qaeda-employee-is-chewed-out-by-his-boss-for-not-filing-expense-reports-poor-job-performance

[13] http://www.timeslive.co.za/africa/2013/06/04/us-offers-23-million-for-aqim-boko-haram-bosses

[14] http://www.bbc.co.uk/news/world-africa-18542030. The leader Abubakar Shekau may have been killed by Nigerian forces during July or August 2013.

[15] http://www.bbc.co.uk/news/world-africa-25187142

[16] http://www.bbc.co.uk/news/world-middle-east-25915607

[17] Barnett (2014).

Groups of Concern Operating in Asia

Al-Qaeda and Associated Movements

Al-Qaeda and Associated Movements (AQAM) is a particularly broad term, incorporating the AQ core and the vast array of groups operating along the Afghanistan/Pakistan border region. The most prominent are the Tehrik-e-Taliban Pakistan (TTP) and Lashkar-e-Taiba (LeT). The latter organisation has been the most open to offering training to radicalised Western citizens to conduct attacks in India, the United States, Europe and elsewhere. The 2006 trans-Atlantic liquid bomb plot provides a clear example. In this case, the plotters were facilitated in their training by Rashid Rauf, a terrorist leader with strong ties to both AQ and Jaish-e-Mohammed. And, like their jihadi counterparts elsewhere, this South Asian group has a willingness to execute mass casualty attacks as evidenced by the 2008 attacks in Mumbai. A 2010 terror warning indicating that LeT or AQ could attempt to hijack an Air India flight illustrates that targeting aviation is not confined to past events, such as at Srinagar airport in Kashmir in 2001 or the Harkat-ul-Mujahideen hijacking of Air India flight 814 in 1999.[18]

Another associated group is the East Turkistan Islamic Movement (ETIM) which is fighting for an independent Xinjiang Province in China but is now largely based in Pakistan's Federally Administered Tribal Areas (FATA). It is this faction that is the critical threat to Chinese interests including the attempted suicide attack on China Southern Airlines flight CZ6901 on 7 March 2008.[19] The unsophisticated plot, as well as the strikes against rail stations in China during 2014, indicated intention to strike but a primitive capability.

Maoists

In India and Nepal, armed groups espousing Maoist ideology also pose a potential threat to aviation. The Communist Party of Nepal (Maoist – CPNM) has placed its military capabilities 'beyond use' and had entered the government, until it collapsed in May 2009. It has a record of attacking aviation infrastructure as it was a critical component of the former government's efforts to maintain contact with the vast parts of the country. In 1994, the group is suspected to have attacked both a Royal Nepal Airlines plane with bombs and small arms as it departed the Chainpur airport and of destroying the air traffic control tower at an airport in Chitwan. More recently, the CPNM threatened to blockade the international airport in Kathmandu during a dispute with the government in October 2009, indicating a continuing awareness of aviation's vulnerabilities.

[18] http://indiaexpressone.wordpress.com/2013/07/25/chilling-story-of-ic-814-hijacking/

[19] Thomas (2011).

In India, the Communist Party of India-Maoist (CPI-Maoist) known as the Naxalites continues to wage a major insurgency based primarily in rural areas of the central and eastern states and is considered the primary domestic security threat by the Union government. The group has not demonstrated any intent or capability to operate against civil aviation but has been able to disrupt Indian rail operations.

Southeast Asian Radicalism

In Southeast Asia, the threats are dominated by ethno-nationalist struggles in southern Thailand and southern Philippines and the religious political struggles embodied by Jemaah Islamiyah (JI), Rajah Solaiman Movement, and the criminal-ideological group Abu Sayyaf. These ethno-nationalist groups have not demonstrated any intent or capability to target the supply chain. JI still infuses a wide range of extremist groups with radical ideology and violent skills to implement their vision of an anti-Western Islamic state. The most violent offshoot of JI is al-Qaeda in the Malay Peninsula, previously led by the now deceased Noordin Top. His death in a raid by the Indonesian Special Force's Detachment 88 in September 2009 exposed a plot to infiltrate airlines in Indonesia. The extent of this targeting and ultimate objective remains unclear. JI has regularly surveiled shipping in the Straits of Malacca, and there was an alleged plot to place mines in the straits in 2010.

The kinetic approach to counterterrorism in the region has significantly degraded the operational capacity of JI and its many offspring. Political negotiations have reduced the level of violence in southern Philippines, and JI has shifted its focus to creating a political and social infrastructure to achieve their ideological objectives. This can best be illustrated through the extensive radical publication and education network among Islamist militants in this region. This quieter phase should not be mistaken for surrender. The ongoing commitment to radical political objectives as well as JI's propensity for large-scale mass casualty attacks, including a 2001 plot to launch a suicide attack at Singapore's Changi Airport, demonstrates that aviation continues to face a significant threat in the region.

Groups of Concern Operating in Europe

The threat situation in Europe has substantially shifted over the last 20 years. The violent ideological clashes of the 1960s and 1970s have all but disappeared. The ethno-nationalist struggles in the former Yugoslavia have ended, the Basque separatist group Euskadi Ta Askatasuna (ETA) declared a permanent ceasefire in January 2011 and the persistent conflict in Northern Ireland has also passed into history, although attacks by dissident republicans remain a serious concern.[20]

[20] http://www.bbc.co.uk/news/uk-northern-ireland-22404582

Despite the increasing threat from dissident republicans in Northern Ireland and a small left wing group in Greece, there is no evidence of a threat to the supply chain. The August 2013 threat from AQ to introduce explosives into civil aviation hidden in breast implants[21] demonstrates a real and continuing threat to civil aviation in Europe. Beyond the well-documented jihadi threat, there is a significant emerging threat from ecoterrorism. In early 2009, aviation had become a particular area of vocal concern for the movement, highlighted by the protests against the new runway at London Heathrow and their takeover of Stansted in December 2008. While the rhetoric has cooled a bit, the drivers remain. The dedication to direct action is widely noted, and if readers remember the long campaign by animal rights activists against Huntingdon Life Sciences, it can be full spectrum and very damaging.

The other key threat in Europe is the Chechen (and related) groups in the troubled North Caucuses. The Chechens have been fighting for independence, on and off, from Russia since 1991. They are noted for their use of mass casualty and female suicide bombers (the so-called black widows) most notably in the twin aviation attacks in August of 2004. The Chechens attempted to spread the insurgency to Ingushetia in 2004 where they attacked an airport as part of a larger operation. The Chechens are accused of attacking Moscow's Domodedovo Airport in January of 2001. As they become more desperate for revenge against Russia and are gaining international attention, the threat to civil aviation across the former Soviet Union remains severe. The February 2013 'toothpaste' warning highlights the innovation of these groups and the continuing desire for a high-profile attack during the Sochi Winter Olympics

Groups of Concern in South America

South America has faced some of the most active pernicious terrorist movements in the world and is home of the premier example of the crime-terror nexus. The threat from the so-called global jihad is more limited and focused on the tri-border region between Argentina, Paraguay and Brazil. Hezbollah has an extensive support infrastructure there and has used it operationally with an attack against the Buenos Aries Jewish Cultural Centre in 1994 and, the following day, by allegedly bombing Alas Chiricanas flight 901 operating a domestic route in Panama. The latter incident is regarded as being the very first suicidal terrorist attack against civil aviation and highlights the primary threat to the supply chain in Latin America is to civil aviation. The details of the February 2013 warning for Americans travelling for Guyana are unknown as of this writing. But the past links Guyana has to Hezbollah require the threat to be taken more seriously. While there is a re-emergence of the Peruvian Maoist Shining Path, the centre of gravity in South America remains Colombia.

[21] http://www.mirror.co.uk/news/uk-news/breast-implants-suicide-bomb-threat-2172911

FARC

The Marxist Revolutionary Armed Forces of Colombia (FARC) is the oldest insurgent group in Latin America and continues to pose a potential threat to civil aviation. FARC has faced a significant reduction in its operational capacity since 2007. The group has been able to survive arrests, deaths and defections of senior leaders due to continued state material support from Venezuela and Ecuador, as well as the late 2009 merger with the smaller National Liberation Army (ELN) and its substantial financial resources derived from kidnapping and deep involvement in narco-trafficking.

The threat to civil aviation derives from FARC's criminal exploitation of aviation as well as its past record of hijackings for political and financial gain. FARC hijacked an Avianca airliner in 1999, taking 41 hostages, while another hijacking of an Avianca aircraft in 2002 led to the kidnapping of a Colombian senator on board. FARC has also attempted to acquire anti-aircraft weapons in recent years, although this is more likely an attempt to develop an anti-helicopter capability against the Colombian army, rather than an indicator of plans to shoot down commercial aircraft.

Groups of Concern in North America

There are two ideological and one criminal threats facing North America. The most pressing of these, once again, emerges from AQ and its metastasising ideology. While there is a concern over independent and semi-linked cells operating in the United States and Canada materialised in the plot against an American passenger train operating in Canada,[22] even lone wolf attacks such as occurred at Fort Hood in the United States in 2010, in which a US Army major shot and killed 13 fellow servicemen, it should be noted that all the significant plots against US civil aviation have originated with attackers from overseas. While this offers some comfort for US domestic security, there are strong indictors that the US-Somali community is radicalising, and it is only a matter of time before this potential threat manifests itself. As mentioned above, with independent cells, there is a higher probability of attacks on groundside operations, particularly in the terminals. The low-cost, high-impact operation is attractive to domestic cells that may not have extensive training in explosives nor the patience to learn.

The second threat consists of the single-issue environmental extremists who, during the last decade, were the most active domestic terrorists and who represent a similar threat to what may emerge in Europe.

The drug war in Mexico is considered a tier one threat to the United States. This is certainly true in the broad sense, but it remains unlikely that the Mexican cartels will use violence against civil aviation as they require access to the system and targeting civil aviation will force an overwhelming response from the United States.

[22] Zennie (2013).

As was seen in Africa, this does not preclude mutually beneficial cooperation but rules out operational targeting.

The drug war in Mexico provides an effective transition to the other threat facing the supply chain, one that is far more common but less frequently addressed by the scholarly community: the criminal use and targeting of the supply chain.

Criminal Interference

There has been considerable professional and academic attention given to the idea of an overlap or nexus between criminal groups and terrorist organisations. The criminal-terrorist relationship is not new; the end of the Cold War – which largely ended state sponsorship of terrorist groups – and the emergence of transnational criminal organisations – fuelled by globalisation and large Diaspora communities – have changed a localised alliance of convenience into a new and worrying phenomenon. The key points of the 'nexus' are that terrorist groups have lost their state sponsorship and therefore need to replace those services (financing, weapons, documents, etc.) to continue their struggle. Criminals can provide all of this for a price. Criminal groups need security and perhaps an air of legitimacy if they are to be seen as helping liberate the oppressed. The key service provided by the terrorists is a weak or at least a distracted state. Criminals need the state to be weakened for their enterprises to flourish. This is the key. Criminals need a state to have sufficient strength to pass and enforce laws, giving the criminals the ability to profit from delivering their illicit services. Terrorists, on the other hand, want to destroy the state so they can replace it. Thus, the internal contradictions over the ends ultimately prevent a true alliance. What may be occurring is a convergence or transference where terrorist groups see the value of profits from the criminal activity and thus will abandon the ideological struggle for a life of crime, while the contact will offer criminal groups an opportunity to gain an ideological orientation and become more political than criminal.

Before discussing the categories of threat below, it is important to note that the biggest single vulnerability in the supply chain is from the knowledgeable insider, along with poor access control and ID badging procedures. Around the globe, there are frequent examples of unauthorised individuals gaining secure areas of the supply chain, such as airside access, and of legitimately employed personnel becoming involved in nefarious activities, including narcotics smuggling.

The two classic examples of this phenomenon are FARC and D Company. FARC started out in the 1960s as an orthodox Marxist revolutionary group in Colombia. With the rise of the cocaine cartels during the 1980s, it discovered new ways of raising finance for its struggle by extorting money and providing protection for clandestine laboratories and airfields. During the 1990s, FARC moved from extorting money to controlling the entire narcotics production network and actually distributing the product in Brazil. The most worrying development is the shift in FARC's narcotics trafficking emphasis from direct routes into the United States to developing their European market through establishing trade routes via West Africa.

D Company, led by Indian crime boss Dawood Ibrahim, emerged during the 1980s, conducting a variety of scams and more violent crimes. During the 1990s, his criminal tentacles reached the Persian Gulf and, at the same time, allegations surfaced of links with the Pakistani intelligence agency, the ISI.[23] He had allegedly begun working with a variety of so-called Islamist radical groups including the LeT (including involvement in the 2008 Mumbai attacks), which led to him being listed by the US Department of the Treasury in 2003 as a proscribed terrorist.

Both of these cases provide some support to the thesis of convergence and crossover between terrorism and criminal organisations. However, criminal groups share many attributes with terrorist groups as violent, clandestine organisations that want to operate much like terrorists. They can also be broken down into the same four categories: linked, semi-linked, independent and lone wolves. The latter two are the most common and, like the terrorists, the least dangerous. The lone wolves are the pickpockets, car thieves and other criminals who are targeting passengers for crimes of opportunity. Lone wolves take advantage of the high volumes of rapidly moving distracted people. This crime of opportunity also applies to most maritime crime, stolen baggage, pilferage of goods and other related issues. This is perhaps the most common issue for staff and other stakeholders in the system, and as a practical matter, there is little that can be done to address the situation. Increased policing and general vigilance are the best tools to approach this common problem.

The independent cells/gangs are organised internally but have no connections beyond themselves. One example is the gangs of panhandlers common to many transportation facilities in the developing world. The 'spontaneous mobs' of children that beg from passengers are in many cases part of a highly organised criminal enterprise whose sole end is to separate the passengers from their valuables. A large portion of the reported piracy incidents fall into this category, where ships and crews are robbed in port, but it is reported as an incident of piracy.

The largest concerns for security and law enforcement officials are the semi-linked and linked cells/gangs. The first case is the semi-linked groups that in the US nomenclature are 'associates' and not 'made members' of a crime family or organisation. The linked are the 'made' men of an organisation. Much of what is traditionally understood as piracy falls into this category.

The preceding discussion began by referring to the current mass violence in Mexico, where four cartels are fighting for control of lucrative smuggling routes to the United States. There are many complex reasons for the recent upsurge of violence there, but one critical element is that the US market for illegal drugs is seen as having peaked or having reached economic maturity. Demand is essentially stable, meaning that all suppliers are struggling to control a fixed market and also being driven to look for newer and richer territories. For the Latin American cartels, that new market is Europe, which is reached by air and primarily by general aviation. The most jarring example of the overlap among criminals, terrorists, state actors and aviation is in West Africa and a particularly notorious example is that of Guinea-Bissau.

[23] http://www.longwarjournal.org/threat-matrix/archives/2010/01/dawood_ibrahim_al_qaeda_and_th.php

The poor, weak West African nation with rampant corruption is a convenient off-load point for narcotics being smuggled from South America to Europe. Once the cocaine is off-loaded, it is transported overland through Sahel into Algeria and Morocco and then across the Mediterranean to Europe.[24] The overland security is provided by Al-Qaeda in the Islamic Maghreb. The primary mode of delivery to Guinea-Bissau and its neighbours is general aviation, in part because it is easier to secure the shipment and in part due to the low level of aviation connectivity to the region.

The above highlights an extreme example of the dangers posed by criminal gangs to both supply chain and the wider political system. But it is the linked and semi-linked criminal organisations, particularly transnational gangs, which have the resources and patience to identify and exploit weaknesses in the system. Irrespective of the activity (narcotics, human smuggling, cash), the supply chain is used to support a range of illegal and so-called 'grey' activities. The most common example of the latter is human smuggling where the passenger has a legitimate ticket but illegitimate travel documents. If the individuals in this situation are identified by immigration authorities, they are expelled at the carrier's expense.

One of the most troubling and least studied issues is direct or indirect infiltration of criminal organisations into the supply chain. There are cases in North America where biker gangs have infiltrated the airports in Canada. The notorious Salvadoran gang MS13 has been accused of influencing the hiring of cleaning staff at some of the most sensitive locations in the US intelligence community. There is no reason to assume that other elements of the supply, which is more directly relevant to their core activities, are immune.

A positive development in addressing the crime-terror nexus has occurred in Somalia, where a concerted international effort has virtually eliminated piracy in this once notorious area. A combination of naval convoy system, shippers changing operating procedures and increased onboard security has reduced the opportunity for pirates to conduct operations. The most important development has been the increasing capacity of the African Union and the government of Somalia to control the ports utilised by the pirates. This has had the added benefit of reducing the funding available to the terrorist group Al-Shabaab, which while not directly engaged in piracy was likely receiving a portion of the ransom paid to the pirates.

Conclusion

The diverse range of threats facing the international supply requires a more dynamic response to address three layers: physical, resource and intellectual.[25] The physical layer of security is the most basic and obvious. There is always a requirement to add more to this layer, but given the current fiscal challenges facing both governments

[24] http://www.spiegel.de/international/world/violence-plagues-african-hub-of-cocaine-trafficking-a-887306.html

[25] Harrison (2011), p 32.

and the industry, this may not be possible. The resource layer requires identifying more efficient ways to utilise existing resources, as well as attempting to identify new ways of evaluating the cost-effectiveness of any additions in the first layer.[26] The most critical and least developed level is the intellectual.[27] The understandable focus here has been on improvements in the intelligence cycle so critical information can be developed, analysed and disseminated to the industry in a timely fashion. The events of Christmas Day 2009, when Umar Farouk Abdulmutallab attempted to blow up Northwest flight 253, despite intelligence agencies having been made aware of him, provide a stark reminder of how a small error at any point in the intelligence chain can have catastrophic consequences. While improvements still have to be made in this area, the main focus should be a greater emphasis on remaining ahead of our opponent. The best way to end the reactionary cycle of security is to develop deeper relations with the academic community, particularly the social sciences. The advancements in research into terrorism and organised crime over the last decade have been very promising. The key development is the growing emphasis on understanding the forces driving innovation within the terrorist and criminal community, thus potentially allowing the security and intelligence services to remain ahead of the trends. This has many potentially positive consequences, but one example is its impact on security technology. The lengthy time required to develop and trial new technologies to meet a specific terrorist threat often results in their being deployed after the threat has shifted. It would seem prudent to invest in more flexible and anticipatory technologies to make sure limited resources are deployed to maximise their impact. Additionally, close relations with the social sciences can avoid fiascos such as the controversy surrounding the deployment of body scanners.

If attention is given to integrating all three levels, we can actually address the key failing identified by the 9/11 Commission, which found that our systems failed not due to a technical weakness but the failure of imagination. A small example of this approach being implemented and working is at some UK airports working *with* rather than removing 'plane spotters' from the end of runways due to the perceived threat. Cooperating with, rather than alienating, these aviation enthusiasts has increased the security in sensitive areas without increasing costs. Similar approaches could be taken with maritime and rail transportation.

Ordinary traditional criminals are a permanent fixture in the civil aviation industry. However, proper procedures to make their operations more difficult will reduce the vulnerability to terrorism. The 2010 cargo bomb plot underscores the continuing attraction and vulnerability of international civil aviation to terrorists. Global terrorism will continue to pose a significant threat to commercial aviation for the foreseeable future. The symbolic value of aviation, matched with the low cost and high impact of an attack, remains a tempting target for terrorists. Terrorist groups espousing Islamist ideologies present the tier one threat to the sector with environmental groups posing an emerging threat, particularly in Europe and North America.

[26] Harrison (2011), p 32.

[27] Harrison (2011), p 32.

Tactically, bombings remain the operation of choice by terrorists. The difficulty of acquiring and successfully using MANPADS limits their operational impact. The emerging threat of operations targeting terminals (bombings and active shooter situations) needs to be addressed. Terminals are the ultimate soft target as they represent the highly desirable combination of high concentrations of poorly defended targets.

The most valuable defence is not necessarily more security but greater intelligence and more rapid, higher-quality analysis and distribution of that intelligence. This perhaps requires the industry to shift away from government and private intelligence providers and look to develop alternative sources of threat information in the research community. But the key trend in the industry is the proper shift in government recognition that crime is an economically motivated activity that can most efficiently be addressed by the industry. Terrorism is a politics by other means, driven not by profit but by ideological goals, and must be addressed by the government. This proper division of labour is perhaps the best trend to emerge over the last decade.

References

Barnett D (2014) Al Furqan Brigades claim 2 attacks on ships in Suez Canal, threaten more. The Long War Journal, 7 Sept 2014. http://www.longwarjournal.org/threat-matrix/archives/2013/09/al_furqan_brigades_claim_two_a.php

Harrison (2011) Terrorism and criminal groups posing a threat to civil aviation. In: Aviation security challenges and solutions. AVSECO, Hong Kong

Mazzetti M, Shanker T (2006) Arming of Hezbollah reveals U.S. and Israeli blind spots. The New York Times, 19 July 2006. http://www.nytimes.com/2006/07/19/world/middleeast/19missile.html

Siddique H (2008) Environmental protests against aviation industry. The Guardian, 8 Dec 2008. http://www.theguardian.com/environment/2008/dec/08/airline-climate-change-protests

Thomas H (2011) Islamist fundamentalist and separatist attacks against civil aviation since 11th September 2001. In: Aviation security challenges and solutions. AVSECO, Hong Kong, p 39

Zennie M (2013) Al Qaeda terror plot foiled after Canadian police arrest two over plan to blow up train to New York as it crossed Niagara Falls. Daily Mail, 22 Apr 2013. http://www.dailymail.co.uk/news/article-2313125/Canada-terror-plot-Authorities-thwart-al-Qaeda-backed-attack-trains-Toronto.html#ixzz33ASzOQjz

Corporate Security: A Supply Chain Program

Mark H. Beaudry

Abstract In today's society, global competition has had an extensive impact on both the private and public sector global supply chain security programs. In addition, security professionals who have previously addressed those conventional issues of supply chain security will now need to ensure that they have incorporated resiliency strategies. In this chapter, the concept of creating and using security processes to assure that the global supply chain security resiliency strategies and emerging threats are recognized is introduced. Also, security professionals in all parts of the world will need to assess the risk on many levels, i.e., the uncertainty of the demand for products locally, regionally, and globally. Unfortunately, many companies still lack experienced security professionals capable of developing and implementing a resilient strategy and using preventative risk assessment tools. Finally, since our global supply chains are vulnerable to a variety of international security threats unlike the past, the uncertainties associated with them now require new security innovations and mitigation measures capable of addressing those emerging risks.

Keywords Security • Supply chain • Continuous quality management • Cargo vehicles • Manufacturing • Theft • Terrorism • Containerized shipping • Security technologies

Introduction

In today's economic environment, many corporations find it challenging to justify security-related investments, simply because they typically view security as a direct expense. Unfortunately, not all corporate security organizations are prepared to take steps to ensure safe transit of their goods across international borders. There are events such as terrorism, natural disasters, product contamination, organized crime groups, production shortages, border closings, or possible strikes at strategic ports that have resulted in the vulnerability of corporate supply chains. This has motivated many corporations to be innovative and develop ways to mitigate risks of such incidents that impact their supply chain. In addition to these types of activities,

M.H. Beaudry Ph.D., C.P.P (✉)
Security Professional, Billerica, MA, USA

A.R. Thomas, S. Vaduva (eds.), *Global Supply Chain Security*,
DOI 10.1007/978-1-4939-2178-2_4

corporations should attempt to find additional ways to achieve organizational resilience. There are various techniques that can be utilized to evaluate their operational schedules, which generally corporations can use to prepare for in advance to mitigate risks: cross-train employees in varied tasks and positions in the event they need to be flexible in their roles, reevaluate the distribution channels and be flexible to change processes in a short period of time, have a preplanned strategy for utilizing substitute parts made at varied locations to spread the risk, and consider the baseline portfolio by location and supplier capabilities. Also, companies can make improvements to their facilities design using *Crime Prevention Through Environmental Design* (CPTED) using protection. This can also address the critical infrastructure to mitigate loss as well as develop a business continuity plan and strategies.

While there are many initiatives that corporations can undertake, they still need to maintain their level of operations while mitigating their risks. Also, see ASIS International, Supply Chain Risk Management Standard (ASISONLINE.org). With that, many corporations are actually beginning to develop a business case specifically to address justifications for major security investments. This is important in order for senior executive management to be aware of the risks and to become better educated and acceptable to investing beyond the minimum baseline security requirements. It is also important for corporations to consider collaborating with their business partners in order to gain support and buy-in from their security-related investments. Furthermore, when developing the business case for supply chain security, organizations should be able to substantiate the valuable benefits for the corporation. The bottom line needs to focus on reducing their vulnerability, via security investments that can show the return on investment. In fact, the primary purpose must be to mitigate risks and make the supply chain secure and less prone to disruption.

Unfortunately, most corporations only came to recognize the critical need to implement end-to-end security after 9/11 for their global supply chain. In addition, this caused many corporations and the US government to adopt varied initiatives to mitigate the risks involved in the transportation of goods. A few of those implemented (Peleg-Gallai et al. 2006) include the following.

First, a requirement that supplies detailed information about the cargo data to the U.S. CBP prior to arrival, known as the Advanced Manifest Rule (AMR). As well as the program that requires the detailed content be sent electronically before the container is allowed into the United States. The Advance Cargo Information (ACI) stated that the information must be sent at least 24 h before the container is loaded on the ship at the foreign port of origin. Second, another program that requires that inspections and screening be conducted at foreign ports is mandated by the Container Security Initiative (CSI). Third, many corporations today are now starting to realize the importance of voluntarily participating in the program known as the Customs-Trade Partnership Against Terrorism (C-TPAT). In return for their cooperation, they are granted reduced inspections at the port of arrival and front of line inspections. Fourth, when the Emergency Planning and Community Right-to-Know Act (EPCRA) was passed, it stipulated that detailed information regarding hazardous materials must be given to the people in the community (Sheffi 2001). Fifth, a program requiring that all low-risk goods be transported only through trusted carriers who have validated trusted drivers are allowed to pass through borders quicker,

as a result of the Free and Secure Trade (FAST) program. Sixth, the need for ensuring that cargo containers are physically secure and their inspection allowed for an audit trail from the place of origin to the final destination is addressed by the Smart and Secure Trade-lanes (SST) program (Hudson 2006). In May 2003, the International Organization for Standardization (ISO) formally set international supply chain security and visibility standards. One of the standards requires corporations to maintain and improve a security management system, critical to security assurance of the supply chain, ISO 28000 (ISO.org).

Roles Specific to Supply Chain Security and Addressing the Key Issues

The World Customs Organization (WCO), developed a Framework of Standards to Secure and Facilitate Global Trade (SAFE Framework), which outlines a strategy that aims to secure the movement of global trade in a way that does not impede but rather facilitates the movement of that trade (WCO 2005). Corporate culture is a key factor in determining the duration and costs associated with a recovery after a major supply chain disruption (Sheffi 2001). Some key ingredients of successful corporate cultures include continuous communication among informed employees – which helps employees make better decisions in the face of unforeseen disruptions; distributed power, so that teams and individuals are empowered to take necessary actions; and passion for work, based on employees' understanding of the importance of their work, which encourages them to be creative in finding ways to overcome unexpected disruptions. Various managerial articles point out the shared cultural traits between resilient organizations such as Dell and UPS (Byrnes 2005; www.ISO.org/) and the importance of management commitment to security measures (Case 2002). In addition to changing corporate culture, companies have also been improving their facilities design to enable faster recovery from natural disasters (Harrison and Malseed 2006).

It is critical for internal security departments to assess ways to address current and future supply chain vulnerabilities and to address the findings in all security standards for internal operations. Those standards could be procedural, physical security, or contractual language that holds the suppliers to a standard. Typically, the security departments will work across all regions and all lines of business.

Efficiency

According to Peleg-Gallai et al. (2006) there are process improvements in transportation and in the customs clearance process. Companies reported the following efficiency-related improvements as a result of their security investments:

1. Improving Product Handling: companies can increase automated product handling by reducing the number of times a product is handled. Such improvements are likely to lower the number of working hours required for these activities, and can reduce the chances for errors in the process or damage to the goods.

2. Process Improvements: companies can reduce the number of steps in their supply chain process, reduce cycle time (measured as the time from order receipt until it is shipped), which is likely to result in higher customer satisfaction.
3. Cargo Inspection and Custom Clearance: most companies can improve many processes in this area to reduce their delayed cargo inspection time, the predictability of these inspections.
4. Speed Improvement: it is important that the just-in-time delivery time window be reduced, also there is the need to reduce the delays during the transit time of all shipping, in addition, a reduction in end-to-end processes are critical to completion.
5. Personnel: by implementing devices such as electronic locks, companies can create a record whenever it is opened or closed, which eliminates the need for employees to escort the shipments, providing a positive return on investment (ROI).
6. Cost Savings: cost savings that can be attributed to speed improvements at the port of entry and in transportation. Such investments in security should be considered as an opportunity for improving business performance and profitability.

Resilience

The relationship between the security measures taken by the different companies and their ability to identify, respond to and resolve problems – especially problems that are related to breaches in security or to delays and other issues companies may face while their goods are in transportation. Reduce the problem identification time, reduce response time to a problem and shortened the problem resolution time (Peleg-Gallai et al. 2006).

Providing Proactive Assessments and the Required Benefit Analysis for Supply Chain Security

The continuous movement of goods, services, funds, and information, are critical to the success of the modern supply chain. Therefore, security professionals must be able to quantify the security measures and any supply chain financial loss that was avoided. Security professionals also need to be capable of measuring the loss of tangible items stolen and any cost of a security breach or disruption. Once again, corporations cannot afford to do nothing to protect their employees, their company, their customers, and the public from criminal organizations. It should be the personal responsibility of every company manager to protect international supply chain. Most corporations also hold insurance coverage for their firm's supply chain being compromised. Preventing the risk of the corporation reputation or any key executives could be irredeemably damaged.

However, in the event of a significant disruption, the corporation's ROI for security is identified through a firm's ability to continue supply chain continuity. Those security professionals with the ability to respond quickly and with resilience to changes will succeed. For example, having the capability to be predictive can build plans will contribute to the corporations ability to operate successfully in a very unstable environment.

Typically, when a security measure does fail, security professionals can calculate the cost of the loss for that particular incident. Most corporate security organizations will have staff that can study the history of security data for supply chain breaches to better understand and predict the cost impact losses on a global scale. Security professionals need to be able to determine their corporations supply chain security losses globally. This can determine any challenges the corporation may face and assist the business to identify and avoid security breaches. Some advancement in this area has occurred and helps security professionals to quantify the benefit from preventing supply chain disruptions. However, additional work is needed to make quantifying the benefits of preventing supply chain security breaches.

Fortunately, there are many opportunities for security professionals to choose from when it comes to technology and methodologies. For example, corporate security professionals can use the Global Positioning Systems (GPS), which allows for the tracking of vehicles and their current locations as they move along. With that, another technology utilized is the radio-frequency identification (RFID) generally used for tracking assets within the supply chain (Rice and Spayd 2005). These technologies have assisted security professionals to identify global supply chain threats and improve practices such as just-in-time and lean inventory processes. In addition, developing programs with local suppliers in order to safeguard against transportation disruptions has been one technique utilized. The radio-frequency identification technology is also used to track container movement while in transit, allow visibility to shippers, facilitate the transfer of information on the contents of the containers, determine the humidity and temperature, seal containers, ensure that it has not been tampered with or opened without authorization, and determine the condition of the containers while in transit (Lee and Wolfe 2003). It is critical that security professionals are prepared to address varied types of vulnerabilities in an effort to reducing theft and preventing loss of inventory. The RFID technology is one potential option that can be integrated into other security processes.

Personnel Security

One of the most fundamentally important aspects of supply chain security is focusing on the "supply" of human resources, which will increase the level of security within the corporation. Personnel security focuses on a thorough initial background check of the potential hiring pool, to eliminate "bad actors." Some corporations also conduct prehiring drug testing as a supplement to the background check.

Primarily, this is one of the techniques used to provide an early warning about employee habits and potential for malicious intent on putting the organization at risk.

Generally, physical security is a common security initiative utilized by corporate security organizations that can improve system security. Physical security will begin with card access system that controls all access of the authorized personnel, while keeping out the unauthorized personnel. Also, the most important security task of any corporate security organization is the protection of personnel, and then other aspects of the business such as intellectual property, capital equipment, inventory, work in progress, finished goods, and product integrity. In fact, most security professionals will establish a baseline level of security that focuses on theft reduction and mitigation of the unauthorized removal of material from the organization. Generally, physical security systems are set at the local site security and determined at the corporate level for global system-wide security.

Corporate Security Standards Development

Corporations tend to develop operating procedures and security standards that direct the global security activities. This may include specific policy statement for investigations, physical security, crisis management, forensics, information security, supply chain security, and business liaison to protect intellectual property. In addition, there may be following guides or process manuals used to respond to incidents of security breaches and methods to improve security systems technology. Also, utilization of any standards previously discussed such as ISO when developing corporate procedures and standards may help reduce security losses through processes and practices oriented toward security.

Developing Supplier Security Relations

It is critical to maintain relationships with suppliers that have established security measures to ensure that your source of material is available to your corporate of supply chain. Also important is the availability of multiple suppliers in the event of a crisis or disruption that one supplier cannot overcome. The interdependencies among multiple suppliers have increased over time, and in today's society, many companies have outsourced parts of their activities to third parties. In addition these have resulted in reliability risks of suppliers, yet less chance of full disruption since many corporations tend to spread their risk through multiple suppliers, hence, limiting one point of failure. Ensuring the supply chains are uninterrupted from end to end is critical to any corporation. As well as ensuring that the integrity and supplier's ability to maintain a supply in a potential security breach is planned for in advance in order to mitigate any potential downtime.

Continued Transportation Security

Avoiding cargo misuse and theft is significant to supply chain security. Using the tools mentioned can help to mitigate theft. Another technique is to use multiple drivers to avoid long stops, hence, allowing the content to maintain a continuous end-to-end transition. Also, as mentioned earlier, using technology to allow for added visibility to all known location and status is important.

Critical Infrastructure and Security Capabilities

Many corporations have made large investments in organizational infrastructure critical to their supply chain security approaches. For most, this is a long-term approach toward increasing their capabilities in the organization through personnel and processes. In fact, the private sector corporations own approximately 82 % of all critical infrastructures in the United States, while the government only needs to secure the rest. Some typical efforts might include providing increased communications systems, building upon employee education so that they are aware of the types of vulnerabilities, and security measures that can be evaluated by performance assessment. This allows for the development of a knowledge base in every employee on security awareness so that they are informed of the broader scope that is well rounded on the broader business needs.

A significant goal for corporations is to tie the role of security to corporate objectives and allow security to be an integral part of business and its delivery of the product or service to the customer. Security should not be a separate activity, because it has much to offer the corporation and may just be the leverage the corporation needs to enhance its supply chain's effort for increased efficiency.

Ensuring End to End Security Operations

Security operations can assist a corporation supply chain through the protection of goods and commodities that present unique challenges as they travel through the supply chain. This was outlined through the work by Closs and McGarrell (2004), who stated that corporations should increase their efforts for greater security into the global supply chain. Furthermore, corporations should develop new security programs to improve the efficiency and flexibility of the supply chain. Their report also underlines the basics for corporations to recognize the comprehensive and integrated end-to-end security processes that elaborate on technology and procedures above and beyond the basics of asset protection. Furthermore, the report recommends that corporations must be looking strategically at security and how security innovations can contribute to the business by developing new processes that give

them as early a warning of possible interruptions. Closs and McGarrell (2004) use a wide-angle lens to describe the ROI of security associated with implementing supply chain security measures. As global supply chain security demands increase, security organizations must effectively meet those demands using a more comprehensive and integrated security focus. A few requirements that the authors Closs and McGarrell (2004) model include:

- How do we develop basic supply chain management and security definitions?
- How do we create a perspective that extends beyond the skills of supply chain security management?
- How do we reassess supply chain security from a critical thinking perspective?

As mentioned, this need for enhanced supply chain security is apparent and the challenge is to reduce the risks and vulnerabilities. For example, a few variables mentioned earlier include research, education, leadership, collaboration with suppliers, and supply chain security management (which includes the application of policies, procedures, and technology) to protect supply chain assets (product, facilities, equipment, information, and personnel). The supply chain security professional should be knowledgeable to conduct self-assessments and create crisis and contingency planning as well as use physical security and technology. The primary focus is that security is concentrated on earlier stages in the supply chain and the identification of key suppliers to increase security through export inspection and information trails. However, there will always be an unexpected disruption of operations; the key is to mitigate the possibility of that potential of impact. The security procedures that are recommended by Russell and Saldanha (2003) as tenets include:

Tenet 1: mutual agreements and relationships with local, state, and federal government organizations are critical to the movement of freight.
Tenet 2: for those global corporations, knowing their overseas trading partners is critical to ensure that they are taking responsibility for securing their cross-border supply chains.
Tenet 3: the ability of corporations to accommodate unexpected delays, interruptions, and disasters.
Tenet 4: being capable of managing a crisis is critical for corporations.
Tenet 5: management of the supply chain in the new environment is necessary for corporations today.

Understanding the New Role of Supply Chain Security

Realistically, both the public and private sector leadership must be capable of transforming themselves to be able to provide a secure and efficient supply chain security process. To do so, they will need to adapt to developing and providing policy direction from corporate, domestically and internationally. In addition, corporations must establish priorities, developing multifunctional teams and

strengthening relationships and the flow of information from remote suppliers to customers. Anticipating the weak links within the supply chain is critical for the global movement of goods.

One of the key components of planning is the "Supply Chain Security Assessment," which the corporation undertakes, is appropriate for use by manufacturers, wholesalers, and retailers. When conducting the assessment for the corporate supply chain security, security professionals need to look at the capabilities and the evaluative characteristics that need to be considered from a number of perspectives. Security professionals must be capable to create and develop key corporate relationships and maintaining processes to enhance security. In addition, security professionals will want to include supply chain security incident management criteria, i.e., planning, mitigation, detection, response, and recovery in all of their continuity plans. Once security professionals conduct a risk assessment, they will be able to gauge the gaps and needed improvements, and ultimately used to develop metrics that can then be used over time to track incidents.

Enhancing Security Throughout the Supply Chain

Using Eastman's (2013) framework, many corporations need to adjust to whatever uncertain economic scenario arises, while supply chain management (SCM) vendors continue to explore emerging technologies and new innovations such as analytics and predictive analytics. The key is to leverage these new technologies such as the cloud and mobility to bring new functionality to their solutions. So, as this technology is adopted, the security professional needs to be an integral part of those practices and activity in order to add value to the supply chain security process. Basically, the key supply chain issues outlined (Eastman 2013) include: (1) *more complexity of the supply chain* – corporations have added more partners to the supply chain, adding complexity. It also has reduced the processing times within the supply chain and this includes integrating new technology as well as adding pressure to deliver more goods and services faster. As we experience the changing economic conditions, businesses must create new models and develop strategies that can meet the expectations of customers. (2) *The real-time supply chain* – with increased Internet bandwidth, today's business is being done faster and more frequently. In fact, security professionals can mitigate uncertainty by sampling demand signals more frequently and more accurately through the real-time supply chain means. Also, corporations have the ability to respond to supply chain changes more quickly and effectively, resulting in cost effectiveness. (3) *Risk management* – risks to the supply chain change by time and location: both man-made and natural disasters can create supply chain disruptions. Also, as technology grows, so does cybercrime and social media exposures to many corporations by varied types of risks. With that, corporations cannot continue to ignore the risks, or the consequences ranging from damage to business infrastructure to disruption to the flow of business and revenue loss, to damaged customer and supplier relationships, or reputation concerns

will occur. (4) *Supply chain continuity* – as consumer expectations rise, any slip-up in the supply chain process becomes more important than ever. As the complexity in the supply chain increases, and the continuous presence of risk needs to be mitigated, the supply chain execution takes on an increasing importance. Finally, paying attention to the consumer expectations, the execution processes are critical to ensure that the product or services get to the customer in an efficient manner. Bottom line, corporations need to assess the "customer experience." It is critical that the customer experience from them placing of their order and concluding with the successful and satisfactory receipt of that good or service be the top priority for a successful supply chain security commitment. This Supply Chain Security Commitment applies to all corporation employees. *Risk Assessment* – companies will need to perform and document an initial security risk assessment of each process that is involved in handling any products to determine site security exposures and improvements necessary to mitigate those exposures. *Physical Security and Incident Reporting* – companies should be able to provide secure facilities constructed of materials that resist unlawful entry and establish internal reporting procedures to report security breaches and concerns to management and/or security, and if necessary to proper law enforcement agencies. *Access Control* – a system that can allow authorized employees to be assigned an identification system for positive identification and access control purposes (this is usually an electronic card). Most technology today can allow security professionals to implement procedures for the issuance and removal of access control devices fairly easily. Also, attention should be given to all areas that are categorized with restricted access to authorized individuals on a business-need-only basis. *Visitor Control Systems* – developing a procedure to monitor visitors (and escort requirements) to areas where corporate proprietary information or products are developed. Most systems today also have contractor and visitor requirements to be identified and to visibly display their temporary identification. *Information Security* – A system should be put into place to maintain procedures to ensure that all information, including documents and computer records, are protected. Ensuring to control access to and limit sensitive information regarding packaging and product shipments to individuals on a need-to-know-only basis. Ensuring that the corporation computer systems use an individually assigned access account that requires a predetermined periodic change of password. Also, implementation of computer security policies must be required and training needs to be provided to employees. A process is in place to assist in the investigation of the abuse of computer systems data. *Procedural Security* – companies will need to implement procedures designed to prevent their products from exposure to security risks. It is also critical to inspect product packaging at both the times of receipt and shipment to verify and ensure that product packaging has not been tampered with. One can reconcile arriving cargo against information on the cargo manifest, including verification of piece counts and labels and verification of weights for inbound cargo on a sample basis or if discrepancies are suspected. Discrepancies will be appropriately investigated and resolved. All incoming packages and mail must be screened before being delivered throughout the facility. *Conveyance Security* – inspection of all empty trailers and shipping containers dedicated to moving products for eventual

cross-border movement, including measuring the interior and exterior length, height and width, to verify that there are no hidden compartments, before loading a product. Once a container or a trailer is filled, then a process of placing an authorized seal for maintaining the integrity of the shipping container or trailer is completed. Security professionals also need to designate where and how containers or trailers are to be stored in order to prevent unauthorized access or manipulation. Procedures must detect report and neutralize unauthorized entry into container or trailer storage areas. *Transportation Personnel – Drivers* – companies should also review procedures with transportation companies interacting with their business. One technique is to ensure that drivers delivering or receiving cargo, packages, or mail present photo identification or are positively identified. Another is to limit their movement within company space; it needs to be clearly defined where they can and where they cannot go within interior space. *Vehicle Seals* – both trailer seals and shipping container seals being used for cross-border movement should meet or exceed the current Publicly Available Specification Organization of International Standards (PAS ISO) 17712 standards for high security seals. *Personnel Security* – put into place processes that screen prospective employees and to perform checks and investigations. As permitted by local law, perform personnel preemployment screening for personnel who will be involved with the company products or who will have access to pertinent data records concerning company products. Security professionals will need to develop procedures for issuing identification, facility access, and system access removal for terminated employees. *Awareness Training and Supply Chain Security Education* – remember to educate the personnel who are involved in processing company products on with responsibility for Supply Chain Security Commitments, including the process for reporting security concerns. Education and training for employee awareness on all threats towards the supply chain is very important. A communication plan should be created to escalate any awareness that security needs to be notified.

The Chief Security Officer (CSO)

Many corporations today are headed by a "Chief Security Officer" (CSO), who must be, first and foremost, be a *businessperson* who is familiar with a corporate environment. Many corporations tend to hire retired law enforcement; however, very few are the right mix for CSO candidates. Some outsiders are capable of quickly learning the corporate environment as well as transitioning into the business mission and objectives.

The CSO is a position in the corporation that creates and develops procedures and plans to ensure that the corporation mitigates risks and can function through those emergency processes in the event of an incident. For example, the CSO office should coordinate awareness through the corporation for all types of crisis situations. In fact, education and training using simulation and optimization models to test various scenarios is one technique used in the security industry. Such models

are readily available and can be adapted to contingency planning in terms of operating partial parts of the business and being capable of responding to different scenarios, and changing conditions.

The CSO's task, however, is much bigger than establishing and testing contingency plans. A Chief Security Officer or security organization will not be successful unless the culture of the corporation promotes a security consciousness to its daily business activities. Efforts aimed at security can actually improve corporate performance and the preparation should be put in place with an eye towards reaping such "collateral benefits." For example, better security measures can help reduce theft, embezzlement, and loss of intellectual property (Sheffi and Rice 2005). The CSO can assist the business with developing relationships with partners and accelerate the work of security standard setting organizations. Sponsorship and participation in the public community security efforts as well as professional associations can also help the corporate image.

Conclusion

Corporations experience risk that has increased dramatically in recent years due to several interdependent trends. Security professionals must cope with the conventional disruptions of supply variability, capacity constraints, parts quality problems (counterfeiting), and manufacturing parts theft. Developing a corporate resiliency plan must be a *strategic* initiative that changes the way a business operates and that increases its competitiveness. Reducing vulnerability means reducing the probability of a disruption and increasing resilience – the ability to bounce back from a disruption. As corporations become dependent on their global suppliers, so does the need for security processes. A corporation's ability to respond to a disruption in one of its own manufacturing facilities with a rapid response involves using preestablished processes and having multiple locations with built-in interoperability (Sheffi and Rice 2005).

Corporations must set high standards for effective security, including compliance with all applicable laws and regulations. Consistent security procedures are critical, as corporations consider their commitments made to governments, customers, clients, and other relationships that are built on trust and responsibility.

References

Byrnes J (2005) Learning to manage complexity. Harvard Business School. Working Knowledge Newsletter, Nov 2005. http://hbswk.hbs.edu/item.jhtml?id=5079&t=dispatch

Case J (2002) Supply chains are tighter but there's still too much slack. Harvard Management Update, 1 Apr 2002

Closs DJ, McGarrell E (2004) Enhancing security throughout the supply. Special Report Series, Apr 2004

Eastman B (2013) Four supply chain issues critical to the success of your business. Inside TEC
Harrison K, Malseed C (2006) Forces of business or forces of nature: building an agile supply network. AMR Supply Chain Executive Conference, Scottsdale, AZ 1 June 2006
Hudson S (2006) Smart and Secure Tradelanes (SST). Supply Chain Resource Consortium, 21 Feb 2006. http://scm.ncsu.edu/public/security/sec060221.html
ISO Web site. http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=41921
Lee HL, Wolfe M (2003) Supply chain security without tears. Supply Chain Manag Rev 7(1):12–20
Peleg-Gallai B, Bhat G, Sept L (2006) Innovators in supply chain security: better security drives business values. The Manufacturing Institute, Standford University
Rice JB, Spayd PW (2005) Investing in supply chain security: collateral benefits. IBM Center for the Business of Government, Special Report Series, May 2005
Russell D, Saldanha J (2003) Five tenets of security-aware logistics and supply chain operation. Transp J 42(4):44–54
Sheffi Y (2001) Supply chain management under the threat of international terrorism. Int J Logist Manag 12(2):8–9
Sheffi Y, Rice B (2005) A supply chain view of the resilient enterprise. Research Future, 15 Oct 2005
U.S. Customs and Border Protection website (2004) Cargo container security: U.S. www.cbp.gov/
World Customs Organization (2005) Framework of standards to secure and facilitate global trade. June 2005. http://www.wcoomd.org/ie/en/press/wco%20-%20framework%20final%20en%2023-8.pdf

An Examination of Global Supply Chain Security Through the Lens of Grid and Group Theory

Jon M. Loffi, Ryan J. Wallace, and Edward L. Harris

Abstract World events such as the September 11, 2001, terrorist attack, the Boston Marathon bombing, and more recently the horrific actions of Boko Haram in Nigeria have put safety and security as top priorities for all people, especially those whose job it is to secure the global supply chain. It is a known fact that obtaining absolute security in any endeavor, let alone the global supply chain, is a chimera. However, security managers endeavor to minimize risks in the daily business of transportation. Conflicting values and organizational inequalities are factors that can severely undermine global supply chain processes. Thus, important issues in risk management concern how individuals and institutions understand, experience, and make choices in reference to certain real or perceived threats. In this chapter, we posit that grid and group theory can be a useful tool to gain insight in conflicting values of risk and the consequences of these conflicting values for supply chain processes.

Keywords Enclave • Fatalism • Grid dimension • Grid and group • Group dynamics • Hierarchy • Individualism • Risk • Security • Supply chain

The events surrounding 9/11 and, more recently, the Boston Marathon bombing and terrorist actions of Boko Haram in Nigeria have put safety and risk management as top priorities in all sectors of society. One of the most vulnerable sectors is global

J.M. Loffi (✉)
School of Educational Studies, Aviation and Space, College of Education, Oklahoma State University, Stillwater, OK, USA
e-mail: jon.loffi@okstate.edu

R.J. Wallace
Aerospace Department, Polk State College, Lakeland, Florida, USA
e-mail: rwallace@polk.edu

E.L. Harris
School of Educational Studies, Educational Leadership - School Administration, College of Education, Oklahoma State University, Stillwater, OK, USA
e-mail: ed.harris@okstate.edu

A.R. Thomas, S. Vaduva (eds.), *Global Supply Chain Security*,
DOI 10.1007/978-1-4939-2178-2_5

supply chain security. The very nature of global supply chains demands that companies exchange valuable products and sensitive information with multiple partners that are often several tiers removed from the manufacturer.

While risk should be a prevailing priority in supply chain management, Bowman (2013) reminds us that most enterprises understand and manage internal risk, but they are not fully aware of the scope and significance of identifying and managing risk across hundreds of thousands of suppliers. This chapter adds insight to this problem because we suggest that organizations do not need to be aware of hundreds of thousands of risk categories that may correspond with companies in the multi-tiered supply process. Rather, we posit that all risks that occur throughout the supply chain can be defined by four and only four categories – individual, fatalistic, hierarchical, and enclave – which will be further explained in detail.

Many definitions of risk include some sort of a probability or chance of the occurrence of an undesirable event. In airport security, for instance, this predictive mindset can be seen in the five-color, threat-level scale, which is intended to reflect the probability of a terrorist attack and its potential gravity.

Defining risk in terms of predictive measures is beneficial in some cases. Because of the multifaceted global society in which we live, risk managers are attempting to address risk in global supply chain entities in terms of culture (Williams et al. 2009; Hudson 2005).

One way to address the culture of risk is to understand risk from the viewpoint of how the different entities in the global supply chain perceive risk. Risk perception is tied closely with risk preference and concerns how individuals understand, experience, and make choices in reference to certain real or perceived threats. For instance, even though the actual likelihood of one getting involved in a commercial airplane crash is minuscule, many people perceive flying as an unsafe mode of transportation. Often, they even opt for other modes of transportation, such as automobile travel, which are statistically riskier than flying commercially.

Moreover, if and when an emergency situation does occur, a person's perception of that situation is vitally important. For example, in his bestselling book, *Deep Survival: Who Lives, Who Dies, and Why,* Gonzales (2004) provides explicit narrative portraits of individuals who do and do not survive extreme emergency situations. His premise emphasizes one's perception is very interrelated with the choices one makes, which in turn has bearing on the outcomes of the situation. In fact, among his 12 rules of survival, *perceive and believe* is at the top of the list.

Accordingly, if risk perception is key in understanding why and how we make choices in security situations, a key question for those interested in global supply chain safety and security is "What are the perceptions of risk among entities in the supply chain process?" The discussion below introduces a theoretical perspective to the field of global supply chain security that explains key dimensions of risk perception and preference.

Grid and Group Theory

The late anthropologist, Mary Douglas, developed a framework that explains how people perceive and act upon the world around them. Referred to as either Douglas' typology of grid and group or simply cultural theory, her model defines risk in terms of social constructs. The framework explains not only *how* individuals and organizations view and act upon risk but also clarifies *why* they actually prefer certain behaviors to others (Douglas 1980, 1992).

Cultural theory explains risk in terms of specific ways of life, which are interdependent with social processes in any given context. In each way of life, specific mindsets are formed that help in understanding one's own perception of risk as well as hinder his or her understanding of another's. Fortunately, in Douglas's frame, there are not endless numbers of "life ways." Douglas posits there are only four distinct contextual constructs, and two dimensions, grid and group, which explain the possible risk perceptions associated with each construct.

Grid Dynamics

In cultural theory, grid refers to the degree to which individual autonomy and actions are constrained by rule and role prescriptions. For instance, in some contexts, prescribed social rules and roles restrain personal freedoms in security activities and interaction, and in other contexts, nominal regulations allow for autonomy in most activities and processes (Harris 1995, 2014).

Grid strength can be plotted on a continuum of weak to strong. At the weak end of the continuum, few role distinctions exist, few regulations restrain autonomy, and individuals are valued for their skills, behaviors, and abilities. In weak-grid settings, members are neither isolated nor insulated from each other by respective role status or labor responsibilities.

At the strong end of the grid continuum, explicit regulations order personal interactions and labor patterns. In strong-grid companies, the workday is governed by rules and protocols that control set times for production and supply chain processes. Pay is often regulated by performance or role, and major decisions are made by upper administration. Strong-grid environments also contain many role distinctions at the lower production and service levels, with proportionately fewer, yet more prestigious, distinctions further up the organizational ladder.

Varying perceptions of risk can be found in both strong- and weak-grid settings. In contexts where role and rule dominate, risk perceptions can differ explicitly among the hierarchical layers. Upper levels may view the social unit as "risk free," as they may be either insulated from hazardous practices that may occur in subordinate rungs or just simply apathetic toward them. Lower-level members' risk perceptions may also reflect the same ignorance or apathy, depending upon their respective role in the organization.

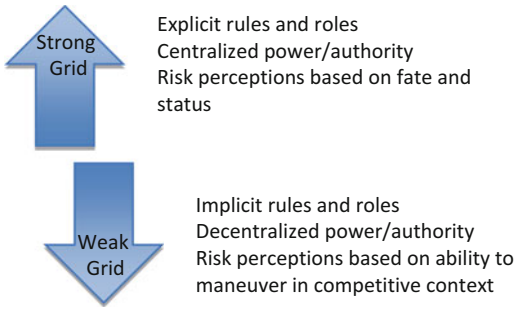


Fig. 1 Grid dynamics and risk

Weak-grid contexts often foster a self-governing mindset. For those in weak-grid contexts, competition and autonomy are dominant values, so risk is a seen as an opportunity for gain. Weak-grid members see risk as a means to capitalize on the better chances while having the freedom to avoid those risks that might result in loss. Some of the salient features of grid can be seen in Fig. 1.

Group Dynamics

In cultural theory, the notion of group refers to the extent to which people are bonded together and committed to the larger social unit. Like grid dynamics, group dynamics are plotted on a weak to strong continuum. Weak-group environments place little emphasis on group-focused commitments, activities, and relationships. Members of working subgroups tend to focus on short-term goals rather than long-term corporate objectives.

An extreme example of weak group can be seen in flea market shops that temporarily set up business in various locations. There are no entrenched traditions, and their business is in constant flux due to recurring site change, employee and/or manager turnover. In these settings, individual interests override corporate goals.

In strong-group settings, explicit pressures influence group relationships, and members are committed to the larger unit. Collective survival is more important than individual survival, and insider-outsider norms regulate group membership. Figure 2 depicts some pertinent features on the group continuum.

Four Risk Mindsets

Grid and group dynamics are simultaneously at work in any setting. Consequently, over time, dominant patterns of thought and behavior tend to define the rules of the game and the way things are done (Deal and Kennedy 2000). However, as mentioned above, it must be emphasized that the two dimensions are spectra, not binary divisions, and each way of life also embraces a particular notion about risk and consequent actions (Fig. 3).

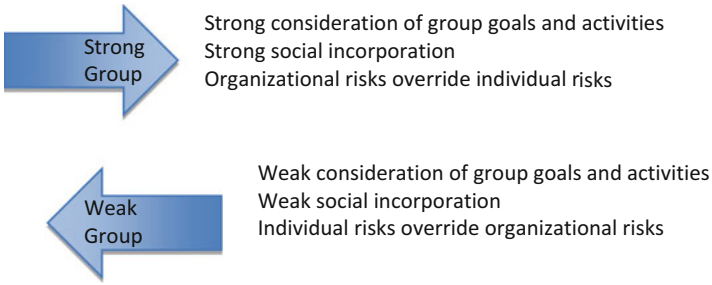
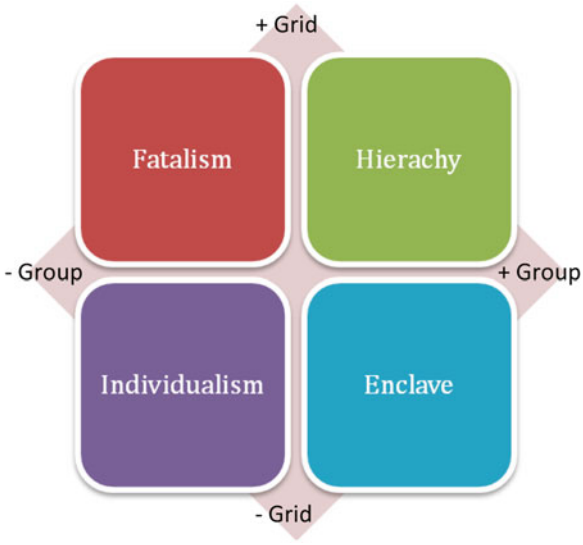


Fig. 2 Group dynamics and risk

Fig. 3 The four ways of life



Individualist (Weak-Grid, Weak-Group) Perceptions of Risk

In individualistic mindsets, civil liberties and independence take center stage. People avoid central authority, accentuate individual differences, and seek self-regulation. Common values of individualists include the following:

- Each individual has a right to protect him or herself; thus, individual survival may override safety in transport.
- A free society can only exist by less governmental restrictions.
- The most intelligent and industrious should receive the most rewards.
- In order to be successful, transport companies must sometimes prioritize economy over safety.
- If one follows all safety regulations and rules, society would come to a halt.

With relatively minimal regulatory oversight, individual-centric goals, and maximum autonomy, individualists could be considered the global supply chain's

"lone wolves." Aside from broad industry oversight, they only follow self-imposed rules. Members of this group are more concerned about individual implications than collective goals. Partnerships are only good if they lead to individual gain. Independent trucking owner/operators are benchmark examples of members of this category.

Fatalistic (Strong-Grid, Weak-Group) Perceptions of Risk

Also known as "bureaucratic," "authoritarian," and "isolate," fatalistic cultures promote minimal autonomy in day-to-day activities, and people are not bonded to the larger organization. There are the "haves" and "have-nots," and both are largely due to role status or fate. Fatalistic contexts offer minimal individual autonomy due to explicit classifying criteria, which emphasize such factors as division of labor and specialization, gender, or family heritage. Common fatalist values include the following:

- Strict rules protect us from accidents.
- Cooperating with and trust of others outside administration rarely works.
- Even if you work hard, you never know if that will help your plight.
- Accidents will always happen because people are unreliable.
- It is unwise to call attention to others' violations of safety regulations.

With tightly controlled guidelines administered under Part 135 of the Federal Aviation Regulations and with little or no group affiliation, one of the supply chain links that fall into the fatalist category is the bush pilot. The bush pilot follows strict rules and conducts operations to remote parts of a particular region, such as Alaska, Northern Canada, or the Australian Outback. Bush flying is a critical link in the supply chain that transports people and goods to areas of rough terrain where seldom is found a prepared landing strip, airport, or other transportation infrastructure. Regarding Federal Aviation regulations, one could reasonably group all Part 135 unscheduled operations in the strong-grid, weak-group category. In the ground transportation arena, freight forwarders also often maintain fatalist traits.

Hierarchical (Strong-Grid, Strong-Group) Perceptions of Risk

Also referred to as "corporate," in hierarchical contexts, group goals take priority over individual goals. Labor, behavior, and relationships are influenced by group norms and social incorporation. This leads to the development of institutions, hierarchies, and laws that both regulate individual action and provide for weaker social members.

Within overall hierarchies, other subcultures may survive. In these contexts, group members understand that in a hierarchical system, what is good for the corporation is good for the individual. Everyone shares opportunities and risks,

but levels of reward and resource allocation are dependent upon placement in the hierarchy. Common values among hierarchs include the following:

- Strong authority and armed forces provide safety to all.
- Within the transport chain, investigators have the right to listen to phone calls and detain information.
- Experts should be trusted to indicate what means of transportation is the safest.
- Accident-prevention regulations and laws are often ignored and broken.
- New technology will solve the problems within transport.
- Proper authorities show sufficient responsibility for safety in the transport sector.

Global supply chain divisions that fall into strong-grid, strong-group categories might include transporters such as Part 121 air carriers, maritime cargo carriers, and corporate trucking companies. Such entities generally have highly structured layers of authority, with clearly established seniority among rank and file employees. Airline pilots epitomize this group, as they are assigned to aircraft, select working schedules, and are paid based on seniority status.

Enclave (Weak-Grid, Strong-Group) Perceptions of Risk

Enclaves are also referred to as "egalitarians," "collectivists", and "sectarians." Enclave contexts have many of the strong-group features of corporate hierarchy, including emphasis on group goals and social incorporation. Conversely, the weak-grid aspect allows for more equitable distribution of resources and fewer role distinctions. Enclaves place high value on unity, equal distribution of resources, suspicion of those outside the community, conformity to collective norms, as well as rejection of mindsets associated with strong grid. Common values among enclaves include the following:

- Fewer regulations and equal treatment of people minimize problems.
- Individualist and strong-grid mentalities jeopardize supply chain security.
- Our group and way of life must be protected at all costs.
- Equal distribution of goods serves the greater good of society.
- When regulations are broken, wealthier companies should get the highest fines.
- Appropriate measures to improve transport safety need not be costly.

While the global supply chain has few transporters, per se, that fall into the enclave category, we do see many sub-corporate groups that meet these criteria. Transportation unions, for example, are often egalitarian in function, as they promote compulsory group affiliation, offer membership security and protection, and are leery of outsiders. Dockworkers also fall into the enclave category.

Cultural theory posits that the aforementioned ways of life – individual, fatalistic, hierarchical, and enclave – and their accompanying beliefs originate in the symbiotic interaction of grid and group and dramatically effect preferences and practices in matters such as risk and other dimensions of social value. Table 1 delineates these four ways of life and their positions toward risk.

Table 1 Cultural categories and risk perceptions

Cultural categories	Risk perception
Individualists	Risk is opportunity for personal gain or advancement; individual security overrides product or group security
Fatalists	In times of imminent threat, regulations and explicit roles protect product and personal security
Hierarchs	Experts and strong government controls best manage risk and protect society; group/product security override individual security
Enclaves	Social equality and equitable distribution are best strategies for risk protection; group security reigns above all considerations

Application of Cultural Theory to Supply Chain Security

As we apply cultural theory to the global supply chain, we see these same variants of organizational culture among the many nodes in the supply chain infrastructure. The collection of trucks, rail, aircraft, or cargo vessels that comprise the global supply chain cannot be viewed equivalently. Rather each of these entities is structured into basic institutional units or companies, and each company has a unique business model and organizational purpose in the supply process. In short, the global supply chain is none other than a collection of varied players that orchestrate individual resources and personnel to transport freight from origin to destination.

A simplified example of the supply chain is overviewed in Table 2. The process begins through the initiation of a shipment, by either an individual or company known as the consignor (Transporteca n.d.). The independent property owner falls into the individualist category and personally bears the risk of loss or profit but is optimistic and perceives this risk as potential for gain. Conversely, the consignor may be a corporate entity and fall into any one of the four grid-group risk categories, depending on the organizational culture.

The shipment is transferred from the consignor to a warehouse, where it is aggregated with other cargo and staged for further shipment. If traveling internationally, the package is inspected and appropriate customs documents are filed in a process collectively known as Origin Handling. A freight forwarder transfers the cargo to a commercial port, airport, or other long-haul transportation medium (Transporteca n.d.; International Civil Aviation Organization [ICAO] n.d.). If affiliated with a company, freight forwarders frequently fall into the fatalist category because of inherent institutional regulations but minimal group attachment. Alternatively, freight forwarding may also be carried out by individual truck owner/operators who operate under their own jurisdiction and are minimally concerned with collective goals, making them distinctly individualistic. Due to their unionization, cargo handlers typically organize as enclaves.

Cargo is loaded and shipped via commercial vessel, airplane, or train and arrives at the destination port of entry (Transporteca n.d.; ICAO n.d.). Most commercial

Table 2 Supply chain stages and risk categories

Supply chain stage	Supply chain entity	Risk category
1. Origin	Shipper (company)	Varies
	Shipper (individual)	Individualist
2. Export haulage	Trucking company *or*	Varies, but often fatalist
	Truck owner/operator	Individualist
3. Origin warehousing	Warehouse workers	Hierarchical organization or enclave laborers
4. Origin handling	Freight forwarding (Company) *or*	Varies, but often fatalist or hierarchical
	Freight forwarder (owner/operator)	Individualist
5. Ocean/airport freight	Longshoremen *or* ground handler	Enclave
	Maritime *or* airline employees	Often hierarchical
6. Destination handling	Freight forwarder (company) *or*	Varies, but often fatalist
	Freight forwarder (owner/operator)	Individualist
7. Destination warehousing	Warehouse workers	Hierarchical organization or enclave laborers
8. Import haulage	Trucking company *or*	Varies, but often fatalist
	Truck owner/operator	Individualist
9. Destination	Customer (company)	Varies
	Customer (individual)	Individualist

water vessels or aircraft operate under a strict corporate mindset. The captain of the ship or aircraft is the head of the chain of command. Senior and junior officers as well as all crewmembers have explicit, hierarchical roles and tasks, which facilitate a unified strong-grid, strong-group system.

At this point, the delivery process is essentially conducted in reverse of the previously described process. Once the cargo passes pertinent customs inspections, a freight forwarder transfers the cargo to a warehouse, where it is uncoupled from its bulk transportation container into individual shipments or packages in a process collectively called destination handling. Import haulage trucks then transfer the package or shipment from the warehouse to the destination (consignee), where the process is completed (Transporteca n.d.).

Cultural theory helps explain the notion of varying risk as it relates to the global supply chain. By categorically grouping supply chain organizations based on common grid and group factors, conflicting values and power inequalities among chain entities as well as strengths and weaknesses in security countermeasures can be identified.

It is worthy to note that the supply chain is rarely operated in a static state. The industry is quite fluid, requiring regular assessment of the corporate culture. Moreover, the supply chain is not conducted in isolation. Organizations often require multiple, diverse supply chains running in tandem to meet complex corporate goals.

The Results Depend on the Magnification of the Theory

The grid-group lens can be refocused and adjusted to categorize various layers of the global supply chain along different macro or micro spectra. We can use the grid-group method as a tool to evaluate the inner workings of a single company as well as to differentiate cultural divides based on various worker functions. Within an airline company, for example, pilots often fall clearly into a hierarchical category, whereas the same company's ground handlers exhibit more enclavist and sometimes, fatalistic, values.

Alternatively, we can zoom out our magnification and use the theory to perceive the social constructs of entire nations or world regions that impact the global supply chain. Cultural theory proponents such as Ellis (1996) and Chai et al. (2009), for example, use the theory to explain broad national and global political cultures and value structures. Thus, one can reasonably adjust the expectations across supply chain entities based on the unique cultural or social norms found in the respective region.

With these general definitions in mind, we can formulate how this method can be used to identify strengths and weaknesses in the global supply chain. Due to the acceptance of best practices, regulation, oversight, and common organizational goals, we may see how stronger grid and group attributes can strengthen security in the supply chain. However, we must be careful not to generalize because terrorist groups such as al-Qaida also operate under strong-grid/strong-group framework.

As opposed to strong-grid/strong-group entities, weaker-grid/weaker-group values are sometimes associated with higher-risk levels. For instance, the individualists' value of self-regulation in risk management is relatively inconsistent. Again, overgeneralization can be misleading because we occasionally find independent operators who are exceptionally contentious and provide good, secure service.

Holistically, regulation coupled with government oversight have proven much more effective, albeit, perhaps not the most ideal solution. While these methods may incur their own scrutiny, it may be appropriate to admit that these methods are merely the best organizational tools we have to date. With these considerations and caveats in mind, we can tentatively infer that supply chain security risk increases as shipments transition from hierarchical and fatalist groups to enclaves and individualist groups.

We can see several examples of this phenomenon when assessing recent major global supply chain security incidents. Perhaps the most notable incident was the Yemen ink cartridge plot. Terrorists were able to introduce suspicious packages into the supply chain at a FedEx facility in Dubai and on a UPS aircraft at East Midlands Airport in England on October 29, 2010. The packages on the aircraft were found to contain pentaerythritol tetranitrate (PETN) high explosives concealed inside printer cartridges. The packages were addressed to Jewish synagogues in Chicago. Some investigators speculated the devices were set to explode inside the aircraft while it was in flight from Europe, and others have said the bombs were designed to explode in Jewish places of worship. The packages were believed to have originated in Yemen,

and intelligence authorities believed al-Qaeda in the Arabian Peninsula (AQAP) were responsible (Macedo 2010). These explosive-laden packages were shipped as standard freight, remaining undetected by the initial collection warehouse and freight forwarder. In both cases, these devices were detected while the strong-grid/strong-group airfreight segment of the supply chain network was transporting the shipment.

In November of 2012, thieves stole a treasure trove of Apple iPad Minis that were valued at $1.5 million from a warehouse at JFK airport. Coincidentally, the same warehouse was the location of the 1978 Lufthansa theft of $5 million in cash and $900,000 in jewelry, which was featured in the movie "GoodFellas." The theft occurred at Building #261 at JFK sometime close to 2300 h. The thieves arrived in a white tractor-trailer, and they pulled alongside the airport warehouse building. Sources reporting on the crime believe the thieves were allowed ingress and egress ostensibly by an insider (Messing 2012). An airport worker discovering the act interrupted the theft and the thieves fled leaving three more pallets of iPad minis. According to NYC Aviation (n.d.), agents of the Federal Bureau of Investigation (FBI) arrested a suspect who had been employed by Cargo Air Services, which operated the warehouse. Again, the security vulnerability, and in this case perpetration of the crime, can be traced back to the weak-grid segment of the supply chain network – the warehouse workers.

In February of 2013, intruders armed with automatic weapons and dressed as police officers in vehicles equipped with blue lights targeted Helvetica Airways flight LX789, a Swiss Fokker 100, awaiting departure at Zaventem International Airport in Brussels, Belgium. Eight thieves cut through a security fence near where the jet was sitting and drove two vehicles across the tarmac and pulled alongside a Brink's van and flight LX789, which was still parked at the jet way. According to Waterfield (2013), the thieves took only 2 min and 50 s to steal $50 million worth of diamonds from the cargo hold of the plane after holding the pilots at bay on the ground outside of the aircraft. Reporters have said this was the most vulnerable time of the cargo just 5 min before taxing for departure. Authorities have since made arrests of suspects connected to the crime in France, Switzerland, and Belgium as the thieves were trying to sell their cache of diamonds on the black market. As with the aforementioned examples, this high-value heist was also carried out during the most vulnerable segment of the diamond shipment, as the enclavist ground crew just prior to takeoff was loading the cargo.

It is important to note that the cultural theory is not designed to assign blame for security vulnerabilities, as there are certainly examples of security weaknesses in all segments of the supply chain. Rather, the theory is designed to point out varying and conflicting values and organizational inequalities, and thereby, provide one other tool to gain insight in conflicting views of risk and their consequences in supply chain processes. Perhaps the greatest value of grid-group theory is that it provides a common vocabulary to discuss these varying views and values across the wide, diverse, supply chain spectrum. Instead of a myriad of institutional structures, we can limit the discussion to four explicit categories. By clarifying the discussion, we can move closer to making the world a safer place.

References

Aviation News @ NYC Aviation (n.d.). iGoodfellas: $1.5 Million in iPads Stolen From JFK [Updated]. Retrieved from http://www.nycaviation.com/2012/11/igoodfellas-1-5-million-in-ipads-stolen-from-jfk/#.U3-4SSjRZ8F

Bowman RJ (2013) Why cybersecurity is a supply-chain problem [Online forum]. Retrieved from http://www.supplychainbrain.com/content/blogs/think-tank/blog/article/why-cybersecurity-is-a-supply-chain-problem

Chai SK, Liu M, Kim MS (2009) Cultural comparisons of beliefs and values: applying the grid-group approach to the world values survey. Springer Publ Company 1(2):193–208. doi:10.1891/1942-0617.1.2.193

Deal TE, Kennedy A (2000) Corporate cultures: the rights and rituals of corporate life. Jossey-Bass, Reading

Douglas M (1980) Cultural bias. Royal Anthropological Institute, London

Douglas M (1992) Risk and blame: essays in cultural theory. Routledge, London/New York

Ellis RJ (1996) American political cultures. Oxford University Press, New York

Gonzales L (2004) Deep survival: who lives, who dies, and why. W. W. Norton & Company, New York

Harris EL (1995) Toward a grid and group interpretation of school culture. J School Leadersh 5(6):617–646

Harris EL (2014) A grid and group explanation of social injustice: An example of why frameworks are helpful in social justice discourse. In I. Bogotch & C. Shields (Eds.), International handbook of educational leadership and social (in) justice (pp. 97–115). New York, NY: Springer

Hudson S (2005) Cultural affects on the global supply chain. Supply Chain Resource Cooperative. Retrieved from http://scm.ncsu.edu/scm-articles/article/cultural-affects-on-the-global-supply-chain. igoodfellas: $1.5 million in ipads stolen from JFK [updated]. 16 Nov 2012

International Civil Aviation Organization, Security and Facilitation (n.d.) Moving air cargoglobally: aircargo and mail secure supply chain and facilitation guidelines. Retrieved from http://www.icao.int/Security/aircargo/Documents/ICAO-WCO_Moving-Air-Cargo_2013.EN.pdf

Macedo D (2010) Bomb materials from Yemen found on way to Jewish places of worship in Chicago. Retrieved from http://www.foxnews.com/us/2010/10/29/authorities-investigating-possible-bomb-threat-philadelphia-international/

Messing P (2012) Crooks steal $1.5M in ipads from JFK. New York Post, 15 Nov 2012. Retrieved from http://nypost.com/2012/11/15/crooks-steal-1-5m-in-ipads-from-jfk/

Transporteca (n.d.). Roles in international transportation: who does what in shipping. Retrieved from www.transporteca.com/transportpedia/roles-in-international-transportation. 26 May 2014

Waterfield B (2013) Target of perfect Brussels diamond heist was cash not gems. The Telegraph, 10 May 2013. Retrieved from http://www.telegraph.co.uk/news/worldnews/europe/belgium/10049033/Target-of-perfect-Brussels-diamond-heist-was-cash-not-gems.html/

Williams Z, Ponder N, Autry CW (2009) Supply chain security culture measure development and validation. Int J Logist Manag 20(2):243–260

Aviation Security and Organizational Behavior

Mohammad Karimbocus

Ink cartridge bomb found on Chicago-bound jet linked to mobile phone SIM card

Daily Mail, 30 October 2010

Abstract The security of the aviation supply chain is fostered mainly by a standard screening system that indiscriminately checks all that is aimed at entering an aircraft. However, the sustainability of this system needs to be assessed, and the time is appropriate to think about revisiting tradition. The mismatch between the rate of aviation infrastructure development and the unrelenting growth in the demand for air travel means airports would be particularly strained for space including the necessary footprint for security processing. Furthermore, as illustrated by events of the recent past, there exists the risk of attempting security breaches from an off-airport environment. An intelligence ingredient (a combination of risk-based methods, observation of behavior, and direct operator-user engagement) to support prescriptive methods of processing would allow for more efficient use of finite security resources. For this purpose, it is essential for an aviation organization to be viewed in a holistic manner and for security to integrate its internal culture. By ensuring that such culture is constructive, security awareness should permeate the organization, and security processing would actually start from the point of initial contact with the user.

Keywords Aviation security • Change management • Organizational effectiveness • Human factors • Leadership

M. Karimbocus (✉)
Avenue John Kennedy, Vacoas 73215, Mauritius
e-mail: mkarim@myt.mu

A.R. Thomas, S. Vaduva (eds.), *Global Supply Chain Security*,
DOI 10.1007/978-1-4939-2178-2_6

Introduction

The occurrence of high profile events in the past resulted in the stringency of security screening being increased dramatically. The consequence of this is that it has become increasingly difficult to perpetrate unlawful acts to aviation directly through airport terminals or airsides.

However, believing that the heightened security screening in airport terminals would result in potential perpetrators of illegal acts to aviation throwing in the towel and admitting defeat would be tantamount to serious complacency. The ingenuity and resourcefulness of such people in their attempts to overcome aviation security should never be underestimated. It follows that going along the aviation supply chain but as remote as possible from airports offers these people a tangible option for breaching aviation security.

Off-airport attempts at unlawful interference in aviation are not exactly new. But past events were predominantly of a military type.[1] The more recent printer cartridge bomb plots are an indication of the degree of subtlety and initiative in the attempted perpetration of illegal acts to aviation.

The Relevance of the Supply Chain

As security threats move further along the aviation supply chain, it becomes necessary to weigh in ways and means to adjust aviation security to cope with these new challenges.

The actual state of things concerning aviation security is that this service is primarily an enforcement function and is therefore viewed from a policing mindset. It operates on a one-size-fits-all basis and in an almost reactive manner involving disproportionate reactions every time a major security event occurs. Such a state of things has a significantly negative impact on the overall efficiency of air transport even though the traditional school of thought would profess otherwise.

In the face of such risks, the traditional response would be to add more stringency to airport security, but this is not the most appropriate option as it would rather add to the already heavy workload of security services. In fact, the strong growth in the global demand for air travel is set to maintain its strong upward trend with around three billion travellers expected for 2014 and twice as much by 2030.[2] Regarding air cargo the forecasts are no less eloquent. The world's two largest aircraft manufacturers estimate a yearly growth of around 5 % for the next two decades.[3] Given that the rate of aviation infrastructure growth can hardly match such a growth in demand, the whole philosophy of airport processes needs a reassessment, and that includes security services. Viewing aviation security solely from a strict enforcement and high-handed

[1] For example, London Heathrow mortar attacks, 1994; DHL Airbus 300 attack, Baghdad, Iraq, 2003.

[2] IATA Director General address, Tony Tyler (2013).

[3] Airbus Global Market Forecast 2012–2031 & Boeing World Cargo Forecast 2012–2013.

perspective would no longer be sustainable and the need to embrace an intelligence-based approach (which comprise of risk-based methods, behavior observation, and other detection techniques for advance identification of ill intent) to supplement the prescriptive methods of aviation security processing has gained prominence lately. The fact that the vast majority of aviation users are absolutely devoid of any harmful intent further adds to the feasibility of new techniques that would ultimately boost the efficient use of limited security resources.

Another very pertinent feature that can be deemed a significant contributor to efficiently secure the aviation supply chain is the advent of off-airport security processing. This is not a new concept but has been promoted since quite some time. It was first mentioned more than a decade ago when ICAO introduced the notion of a *regulated agent* (*defined as an agent*, *freight forwarder*, *or any other entity who conducts business with an operator and provides security controls that are accepted or required by the appropriate authority in respect of cargo or mail*) in 1997 in the 6th edition of Annex 17 to Chicago Convention. Thereafter, the concept was furthered with the notion of the *known consignor* (*defined as a consignor who originates cargo or mail for its own account and whose procedures meet common security rules and standards sufficient to allow the carriage of cargo or mail on any aircraft*) which was introduced in the 9th edition of the same document. Since ICAO contracting states have the obligation to implement all annexes to the Chicago Convention into their national legislation, the consequence of these updates to Annex 17 is that national aviation security legislations apply to qualified cargo agencies and other stakeholders with access to aircraft (including appropriately vetted originators) in addition to operators of aircraft, airports, and air navigation services.

These inclusions in ICAO Annex 17, which confirm that aviation security screening should not be solely confined to the airport environment but needs to be moved along the aviation supply chain as well, are fully justified. The proper application of remote security processing has the double potential of firstly generating significant efficiency in the provision of aviation security services and secondly to provide the ability of addressing off-airport attempts at the breach of aviation security. Events of the recent past have illustrated the subtlety of such attempts, and it is important that they are identified well ahead of reaching the airport environment.

Regulatory Requirements

By definition, regulated agents and known consignors have to comply with aviation security legislation and are subjected to the same regimes of regulatory oversight as airport-based security services. This implies that they should possess the appropriate logistics and human resources to safeguard civil aviation against acts of unlawful interference.[4]

[4] ICAO Annex 17: Definition of security.

Benchmarking on Airports?

Conventional wisdom would point to benchmark on airport-based traditional security services for the acquisition of logistics and other resources. However, there is a big nuance between airports and these entities:

- Airport security services have perpetuated the legacy of a high-handed and uniform method of operation that has paid very little regard to efficiency and that has always added more stringency as reaction to security events. This traditional form of aviation security has survived the transformation of airport operators into more business-oriented organizations.
- Airports are hubs in the global supply chain and as such handle substantially larger volumes of cargo that any single freight forwarder. Acquiring the same level of logistics and human resources would be daunting for even a large-scale cargo agent.
- Airports are highly secured areas with different layers of controlled access culminating into a security restricted area comprising of the airside and sterile zones.
- Airport-based security filtering is generally perceived as a routine step leading to air travel and thus has a high level of predictability. On this issue it is therefore not fortuitous that in its latest proposed amendment[5] to Annex 17, ICAO has introduced the notion of unpredictability whereby for the purpose of increasing the potential of security controls to deter illegal intents as well as to promote efficiency, the frequencies and locations of their application as well as the means to achieve them should not follow a defined pattern so as to eliminate its predictability.
- A risk-based approach which implies advance profiling, and dissemination of information, works on the premise of advance knowledge of the intention for air travel. This might have limited significance for off-airport regulated agents which are in reality the first interface between the user and the supply chain. Also, privacy and data protection issues might preclude the dissemination of sensible data to private entities.

Efforts at revamping aviation security processing have been ongoing for quite some time. Along with risk-based security profiling, the development of techniques for behavior detection is the most prominent novelty to be introduced during the recent years. But, while observation techniques have been applied in passenger terminals, their application for cargo security would need some specific adaptation. However, the effectiveness of behavior detection by observation has been put into question in the USA. The report of the US Government Accountability Office in

[5] ICAO State Letter AS 8/2.1-13/58: Proposal for amendment of Annex 17 circulated July 2013; scheduled to be applicable late 2014.

2013[6] has cast doubts on the ability of the Screening of Passengers by Observation Techniques (SPOT) program to effectively identify persons who pose a security threat to civil aviation.

The other method of behavior detection, namely, verbal detection which involves direct interaction with users is deemed as having greater potential for identification of security threats, but in the absence of a definite curriculum and guidance for acquiring the relevant competencies, it would be difficult to implement on a significant scale.

On the global scale, risk-based security may still be presumed to be in its infancy, but it is already legally in use in the USA, albeit not yet on a large scale[7] and is poised to gain global significance. As stated by the Administrator of the Transportation Security Agency (TSA) before the Subcommittee on Homeland Security of the US House of Representatives Committee on Appropriations (February 2013), the USA is intent on expanding the use risk-based security. It can be presumed that in due course the global aviation body would follow by calling for its worldwide implementation.

Whatever way security is looked at, the key is about the proactive identification of risks for illegal acts. Therefore, the objective should always be an aviation supply purged of all illicit or noxious materials and ill-intentioned persons.

Security and Efficiency

Regulated agents and known consignors are primarily business organizations and are under the obligation to strive for resource optimization in the conduct of their activities in order to be viable while at the same time being on the right side of security legislation. This reasoning also applies to airports and other aviation entities which support their operations through user charges. Perpetuating traditional aviation security processing would make it very difficult to reconcile security and efficiency.

The assurance of the coexistence of efficiency and security should be the goal of any organization linked to the aviation supply chain though this would be difficult to envisage for the traditional mind. But it is imperative that these are reconciled for the long-term benefit of the air transport industry. The prescriptive mindset (whereby security people are "oblivious" to the notion of efficiency and conversely other sectors within an organization are not concerned with security) which tends to display security and efficiency as antipodal should mutate into a more holistic way of thinking (the "know-your-neighbors" attitude). This is not a new concept in that ICAO has, for more than two decades, been promoting the notion of efficiency[8] at par with safety and regularity in the implementation of aviation security processing systems.

[6] GAO Report to Congressional Requesters, November 2013: Aviation Security.

[7] For example, Risk-Based Security Screening for Members of the Armed Forces Act, January 2012.

[8] An ICAO standard since the 3rd edition of Annex 17 (March 1986).

The Evolution of Security Technology and Its Limitations

Technological progress has resulted in a quantum leap in ensuring supply chain security. While a significant level of technology has been aimed at preserving consignment integrity and monitoring along the supply chain (e.g., the smart container concept, electronic seals, RFIDs, etc.) to prevent pilferage and tampering in transit, there has also been enormous progress in scanning capability for the detection of illicit materials.

Regulated agents and known consignors would definitely have to invest in screening technology the extent of which would depend on the specifics of their business.

However, technological progress in security scanning could be very onerous and would inevitably require a long lead time for development and implementation. And most of the time, it is reactive in that its implementation would mostly be "after the event." After all it would be utopian to think of the complete scanner which could uncover all types of illicit matter be it chemical, biological, nuclear, radiological, or even the conventional explosive. And aviation would have to live with failed screening and false alerts and their impact on general efficiency.

Also, notwithstanding global protocols that have come into effect, such as the Protocol for Marking Plastic Explosives, the risk for illegal fabrication of noxious material will always exist.

Yet another downside of technology is the fact that there could be a significant negative impact resulting from indiscriminate screening on the aviation supply chain.

The Central Role of the Human Component and the SHELL Concept

Based on the reliability of scanning systems, it would be very tempting to think that this service is primarily technology driven. This is an erroneous belief because while technology might enhance screening, decision making based on such scanning is a human responsibility. Moreover, accountability for any breach in security screening shall ultimately rest on the human component. This leads to the reality that the human is central in the aviation security system. To further comfort the central nature of the human, Schwaninger (43rd ICCST, Zurich 2009) talks about screeners rather than screening equipment failing covert tests.[9]

In safety-critical aviation services where there is substantial use of automation, the central nature of the human element has long been acknowledged as illustrated by the SHELL model. Present-day aviation security also relies significantly on technology which is constantly getting more reliable. So the SHELL model can also be highly relevant to this service.

[9] Schwaninger (2009).

The SHELL Model

Originally conceived as the SHEL model (Wiener and Nagel 1988), this concept works on the premise that the human component is rarely the sole cause of safety issues even though they occur as a result of (inappropriate) human decision making (the major exceptions being direct operational errors and violations).

The human component or liveware (L) is at the center of all activities, and the SHEL model lays emphasis on human interaction with the other components, namely, hardware (H), software (S), and the environment (E). Considering the inevitable interaction of the central human component with a peripheral human component (e.g., ATC-pilot interaction), the SHEL model evolved into the SHELL concept (Hawkins 1984 in ICAO Circular 216).

The liveware is considered as the most critical element of the SHELL model which emphasizes on its interaction with software, hardware, environment, and (peripheral) liveware. While the flexibility of the liveware is clearly established, its limitations for information capture and processing capability are equally well known. Furthermore influences such as social, psychological, and physiological pressures have a direct bearing on human performance.

Software in the context is much broader than software for computer hardware. In the SHELL model it also represents all intangible elements such as laws, rules and regulations, procedures, standards, habits, conventions, and so on.

The hardware component consists of all physical buildings, tools, equipment, materials, displays, seating, and so on.

Work areas, lighting, ventilation, noise, and temperature are the major constituents of the environment in which the liveware operates.

The SHELL model is an analysis tool for human behavior in complex systems. It is meant to foster safety by focusing on the interaction of the central liveware with the software, the hardware, the environment, and the peripheral liveware. It is not concerned with software-hardware, software-environment, or software-environment interaction.

In a nutshell the SHELL sheds light on the issues bearing on human behavior and thus allows for better human performance.

Performance Versus Compliance

The obvious inference of the preceding discussion is that all other stakeholders linked to the global supply chain should comply with aviation security regulations in the most efficient manner possible. By virtue of the central nature of the human component, the first need is to look at human resources.

Technical and operational competencies shall be imperative at all times. But the changed nature of present-day operating conditions has imposed additional requirements to the human resource, especially when the focus is on the long-term

sustainability of air transport. These additional requirements can only be identified by properly assessing these operating conditions.

The most appropriate benchmark for this purpose is the field of aviation safety where the quest for safety performance (as opposed to traditional strict safety compliance with no regard to efficiency) was initiated about a decade ago.[10]

Safety Management: The Organizational Culture Path

The concept of managing safety (or performance-based safety compliance) originated from the fact that the traditional prescriptive safety compliance methods were seen as unsustainable as a result of both worsening economic conditions and the ever-growing use of automation in aviation. The most appropriate definition of management being *the process of getting activities completed efficiently and effectively with and through other people*,[11] it becomes evident that the ultimate objective of safety performance is to achieve efficiency. At this stage, any perceived worries that this is an "invitation" to cut corners need to be allayed. The nature of civil aviation as a mode of transport means that compliance with safety standards as defined by appropriate regulations and other legislation shall forever remain a sine qua non. Safety management is about bringing resourcefulness in optimizing the use of resources for achieving such compliance.

Taking an analytical look at the concept of safety management, it can be realized that it relies significantly on the premise of advance knowledge though it does have a reactive part to deal with previously unidentified failures. It is mostly about advance identification of safety risks and the formulation of elimination, containment, or mitigation strategies in an equally proactive manner.

From a safety performance viewpoint, safety occurrences are classified as active failures (occurring at operational level and potentially having direct adverse impact) or latent failures. However, active failures may not always occur as a result of violations or errors on the part of frontline personnel. The notion of latent failures arises from the fact that in complex systems such as aviation which have multilayered safety defenses,[12] safety breaches rarely occur in isolation and are more often the consequence of triggering conditions "further down the line." The underlying philosophy is that by looking at the causation rather than the cause of safety events, it is possible to preempt active failures resulting from latent conditions and thus bring efficiency in the compliance with safety standards. Put otherwise, instead of asking why do operational personnel make safety breaches (the cause), the question should be why do primarily competent people make decisions that end up in breaches of safety (the causation).

[10] ICAO Strategic Objectives 2005–2010 (Strategic Objective A, Key Activity A8), December 2004.

[11] Stolser et al. (2011), p 18.

[12] Reason (2013)

The salient element of this reasoning is that safety need not be viewed as the sole responsibility of the frontline or operational human component. By considering aviation as a mode of transport and therefore inherently targeting safety of users and third parties, it is evident that this reasoning makes sense because all departments within an aviation organization ultimately contribute to the common good, namely, safety.

The expanded view of safety responsibility leads to the notion of organizational culture. This is very sensible actually because safety events based on technical deficiencies and individual human behavior have been very significantly harnessed since quite some time. Nowadays, safety events are viewed from a broader perspective where organizational factors are deemed contributory to their occurrence. The term organizational accident is a very apt illustration of this concept.

The central role of the human component is preserved under any circumstance, and thus the organizational approach also focuses on human behavior. The difference is that this behavior is not focused on the human as an individual but as being part of an organization. It is that relevant to note that nowadays there is mention of the SCHELL model as an evolution of the SHELL model with the C component standing for culture.

Envisaging the adoption of an organizational approach similar to that of safety-critical services has enormous potential for efficiency in the provision of aviation security. The approach to this should start with the premise that security compliance is the focus of the whole workforce within an organization rather than being solely confined to screeners and other personnel directly implicated in detection or security management. But the ultimate objective is appropriate human behavior on a broader scale.

Aviation Security and the Human Component

The SHELL model was conceived primarily for safety-critical services. Aviation security also employs a significant level of automation especially as screening tools and as such human-machine interaction is just as relevant. On the same note, techniques for observation, interviews, and other profiling techniques point to liveware-liveware interaction. Therefore, adapting the SHELL model in aviation security is highly relevant in the quest for efficiency.

However, just like comparing art with science, there is a nuance on the issue of data acquisition and human decision making in aviation security as compared to safety-critical services. In the latter services there are definite parameters for use as benchmarks for data interpretation to indicate a safety breach which would trigger an alarm. This is not exactly the case with security services. The inherent limitations of screening technology compounded with the packaging complexity of consignments and the ruse employed in concealing banned items mean that security operators need to supplement machine-based screening with their own assessments. This requires a high level of individual capability and mental ruggedness which can only be obtained through training and enhanced through sharing of knowledge and experience. This specificity of aviation security adds further relevance to the need for an organizational approach within aviation entities that are linked with security compliance.

The Organizational Approach

The endeavor to embrace an organizational approach for the provision of aviation security requires, at the outset, a proper understanding of the meaning of an organization and, by extension, organizational culture and organizational behavior.

The organizational approach to the provision of aviation security services requires viewing the organization concerned from a holistic perspective rather than considering it as the sole responsibility of the security department. The meaning of this is that every unit within the organization contributes to the "common goal" which is the prevention of illegal acts to civil aviation. Based on the central nature of the human component in any activity, the organizational approach focuses on human behavior within an organizational setup (as opposed to a stand-alone or insular behavior) and promotes an inherent collaborative environment.

The concept of an organization arises from the reality that practically all activities have superordinate goals[13] and as such inevitably need to group together people with diverse skills and competencies to achieve such goals. Conventional wisdom would lead us to believe that each department within an organization would operate in some sort of stand-alone manner. However, the reality is that the effectiveness and efficiency of any activity hinges on the orderly and organized interaction between the various human components. This leads to the notion of organizations where these diverse human components with a variety of appropriate skills and expertise operate collectively under a given structure to "produce" the common good. A very appropriate definition of an organization is given by Keyton who states that it is "a dynamic system of organizational members, influenced by external stakeholders who communicate in a purposeful and ordered way to achieve a superordinate goal."[14] In somewhat simpler terms, Schermerhorn, Hunt, Osborn, and Uhl-Bien define an organization as "a collection of people working together in a division of labor to achieve a common purpose."[15]

Organizations have clearly defined goals which they aim to achieve by operating within sets of rules and regulations and based on their own culture. Organizational culture is based on artifacts, espoused beliefs, and values as well as basic underlying assumptions[16] and is dynamic. It influences the human component and by extension also bears on how the organization achieves its objectives. It would not necessarily be the same for two entities doing the same business and is influenced by the reality of a mutating workplace, the advent of new ideas, the quest for new opportunities, and so on. The assumption is that the prevailing organizational culture permeates an organization (the "here-we-do-it-this-way" attitude) and determines organizational behavior which is the behavior of the human component within the organization. Moreover, new recruits being inducted into an organization are expected to embrace

[13] Keyton (2011, pp 6–7).

[14] Keyton (2011, p 11).

[15] Schermerhorn et al. Organizational behavior, p 8.

[16] Schein (2010). p 24.

the prevailing organizational culture. Within entities linked to the global aviation supply chain, the adopted culture is expected to generate security awareness among non-security personnel and conversely should help security people to acquire an appreciation of the notion of efficiency. For this to be possible, a constructive culture is most conducive as opposed to passive or aggressive cultures.

Every organization linked to the aviation supply chain can be viewed as a node through which "traffic" (people and consignments) is fed into the chain. Each such node acts as the interface between the outside world and the secured aviation supply chain, and three of its major objectives are:

- It must foster its own viability as a business entity by operating in the most efficient possible manner.
- It must contribute to the efficiency of the actual patron of the air transport industry through ensuring timely transits and arrivals.
- It must have in place all security defenses for the protection and integrity of the aviation supply chain against all risks for illegal acts.

From a purely simplistic standpoint, these objectives would seem unrelated and are only achieved in isolation. But the reality is that they are inherently intertwined. This becomes evident when taking a systemic view of a node linked to the aviation supply chain. Just as tributaries feed rivers, every organization (or node) has in place its own system of internal flow or sub-supply chain to ensure the seamless, efficient, and secure transit of consignments between the outside world and the aviation supply chain. An organization's business and compliance viability is heavily influenced by the "health" of this sub-chain which by extension also affects the aviation supply chain.

The establishment and functioning of a tributary to the aviation supply chain is internal to each organization concerned. This brings in the relevance of a company's organizational culture with focus on the organizational behavior of its human component.

Integrating Security into Organizational Culture

An organization's internal sub-chain starts from the point of first contact with the user. This is the level where the potential for detection of deceit (concealing ill intent) is the highest. From a holistic perspective, this should be in actual fact the first security layer as consignments transit into broader aviation supply chain. This requires that an organization integrates security into its culture through ensuring broad-based security awareness and setting up a clearly defined internal line of communication for the proactive dissemination of security-related messages generated at the point of initial contact.

The first prerequisite for promoting organization-wide security knowhow is to operate a paradigm shift in the way aviation security is viewed. Rather than perceived as a purely enforcement service characterized by high-handedness and indiscriminate (and ritual-like) screening, it should display a hassle-free image and have

an inherent intelligence component. This can be a challenge since a security department may have a "protecting-its-turf" attitude (akin to an aggressive/defensive subculture) and might either be unwilling to open up or would simply promote the traditional enforcement mindset to other sectors of its parent organization.

Behavioral aspects of the human component with regard to security compliance are the next area that should be analyzed. As in all activities, the human operates by following the standard pattern of data acquisition, brain stimulation, data analysis, and decision making except that in aviation security, the human operates in real time just like in all transport-related safety-critical services.

In aviation security processing, data acquisition means the identification of the potential for illegal acts whatever the technique used and also incorporates a high dose of flair on the part of the security operator. Ultimately, decisions would be taken upon the assurance that the most appropriate analysis of the acquired data has been made.

While the need to operate in real time requires specific character traits, there is yet another aspect that bears heavily on the psyche of aviation security personnel: the huge psychological effect of security events. It is therefore imperative that human resources at the various layers of security processing are appropriately groomed and possess all the competencies, character, and resilience to withstand the rigors of their operating environment. The best efforts should therefore be made to ensure that security operators attain and maintain cognitive capabilities, emotional intelligence, and psychological ability to detect deceit beyond a determined threshold that is proper to their rigorous work environment. Beyond these qualities, adherence to the prevailing organizational culture should also become a constituent part of human resource competency acquisition.

Cognitive Skills

The subject of cognitive capability has been widely documented, but it is especially relevant in the high-stress, time-constrained environment of the safety-critical and security-sensitive areas of the air transport industry. In addition to real-time decision making, screeners are required to process bags and other consignments of varying packing complexity and at the same time should ensure that false security alarm rates are kept as low as possible. Cognitive strengths should be particularly appropriate so as to ensure that the ability for decision making based on logical analysis of data is not impaired. It is worth noting that at Section 3.1.2 of ICAO Document 9808, it is clearly mentioned that security operators should operate the screening task for periods of 20 min.[17]

[17] ICAO Document 9808 (2002).

However, in an organizational setup, security operators would have an important boost to their cognitive functions by having advance knowledge of security issues through the proactive notification of risks identified at preceding processing positions.

Emotional Intelligence

While cognitive skills are essential, these would not suffice for optimum human performance. The human species is especially susceptible to emotions (whether positive or negative) which are ever present in any environment. Taken within an organizational setup, it affects internal communication and interaction (if hierarchy considerations are taken into account, it actually controls it) and thus influences organizational culture. Emotions have an impact on rational thinking and as such inevitably have an impact on human performance. Goleman[18] has stated that the human has "two minds; one that thinks and one that feels" and further avers that these two minds are "exquisitely coordinated" under normal conditions. Taken in the proper context, this means that emotions can actually help in rational thinking, except when passions surge and the emotional mind takes the upper hand. For sustained high level performance, the key is to be able to curb any potential for the emotional mind subduing the rational mind. This can be achieved through developing and enhancing the human emotional intelligence (EQ). The purpose of emotional intelligence is to ensure that the human understands and makes positive use of its own emotions as well as of those within its surroundings so as to relieve stress, meet up with challenges, and avert conflicts.

This facet of the human character is defined as the ability of understanding and dealing with one's own emotions as well as of those in immediate surroundings and to behave in such a manner that preempts any risk of emotions getting the edge over the rational. This can be achieved through perfecting self-awareness, social awareness, self-management, and relationship management.

Self-management deals with understanding personal emotions and their impact on others as well as on the immediate vicinity and other stakeholders. Social awareness is about being empathizing with others and understanding their own emotions and also their impact on relationships. Self-management skills enable the human to stay in control of its emotions and to have the "think-before-you-act" mindset. It helps curb impulsive action. The ability of building good relationships with others as well as making positive use of their emotions is known as relationship management.

Emotional intelligence can bring forth substantial efficiencies in aviation security provided that it is correctly used within an organization. Taking into account time pressures and that even one security event is one too much; personnel having a high level of emotional intelligence to supplement their cognitive ability are better prepared to reconcile security and timeliness and thus efficiency.

[18] Goleman Emotional intelligence.

Detection Abilities: Identification of Deceit

Aviation security operates on the premise that the potential for illegal acts is detected and addressed ahead of air travel actually taking place. Traditionally, the detection function comprises of machine screening of bags and other consignments along with walk-through X-rays and frisking for passengers though observation techniques may be in use in some places. The limitations of such procedures as well as their effect in terms of perceived harassment and on the fluidity of the aviation supply chain are well known within the air transport industry. This provides ample justification for the need to inject an intelligence supplement that would effectively contribute to streamline security procedures.

An intelligent security screening system would start with exploring the origins of illegal intentions. First and foremost, these are by definition premeditated and as such the perpetrators are inevitably under the effect of some kind of emotion while trying to use deceit to move illicit materials into the aviation supply chain. The ability to identify such deceit provides the best opportunity for injecting intelligence into aviation security. It is thus important that such ability be developed, maintained, and continually enhanced. However, it should be appreciated that this is not a straightforward endeavor as persons animated with ill intent would most probably be of the mentally rugged type and very skilled at concealing their emotions and have confidence in their ability to overcome security screening.

The detection of intents for security breaches can be through observation of body language, voice, language, facial expressions, and so on. According to Ekman,[19] studies have shown that while a very high level of accuracy can be achieved through measuring multiple behavioral parameters (90 %), observation of facial expressions alone generated a 70 % accuracy level. On the issue of developing detection ability, Ekman has further stated that the emotional effect of concealing lies is mostly displayed by micro-facial expressions that last a very small fraction of a second. This would easily evade the attention of the inadequately trained operator and makes training requirements even more stringent. Therefore, training in behavioral observations[20] aimed at detection of deceit should be promoted as an essential feature for personnel linked to the aviation supply chain. Furthermore, the development of skills for verbal engagement with users on initial contact for identifying inappropriate intent should also be an inherent element of such training curricula. Being deemed as the first security layer, the point on initial contact of the user (i.e., the cargo consignment drop-off point or the passenger registration counter in airport terminals) is an especially appropriate spot to apply deceit detection techniques to help foster efficiency in aviation security. Detection at the first encounter between the user and airline/airport staff would enable ensuing security stages to have advance information and thus generate the potential for streamlining the ultimate security filtering process.

[19] Ekman (2009).

[20] For example, Dr. Paul Ekman's METT Training Tool.

Practical Application of Organizational Culture: The Constructive Culture

Organizational culture is inherently present in any area of activity. Tangible benefits could only be obtained if its real meaning permeates the organization concerned and the most appropriate culture is adopted. Such culture should pragmatically promote a collaborative mindset and mutual respect and discourage critical, competitive, or confrontational attitudes. These are achieved through nurturing an organizational culture which makes the human component behave as having collective ownership and aiming for the common good. However, two pitfalls should be avoided. Firstly, any constituent part of an organization (especially at the higher echelon) may unknowingly be tempted to have a sort of pseudo-culture by putting its interests above those of other stakeholders despite claims to the opposite. This could ultimately generate mistrust and segmentation within the organization. Secondly, it may happen that higher management has the most appropriate culture, but the rest of the organization has not been inculcated with these values and behaviors. It is essential that cultural values pervade the whole organization and the more so at the operational level. This requires a learning process right from being inducted into an organization.

The most appropriate culture that would reconcile security and efficiency is the constructive culture. This type of culture has all the characteristics that would allow for efficient production and service delivery. Its major trait is that it is focused on the human component through being self-actualizing and humanistic encouraging. This instills a feeling of collective ownership of the organization rather than working under fear or coercion. People are encouraged to be creative and spontaneous thus becoming aware of their own potential and at the same time being keen to go the extra mile. In parallel, this culture promotes the notion of people mutually helping each other. In addition to self-fulfillment, the human also develops consideration for others and is inherently predisposed to help others progress. The generation of mutual understanding, collaboration, and cooperation thus created provides the most compelling work environment for the human to thrive and operate to its full potential. The ensuing benefits to the organization cannot be underestimated.

The application of a constructive culture for the security of the aviation supply chain lies on a very straightforward premise: an organization involved with feeding this supply chain (be it an airport, a regulated agent, or a known consignor) should operate with the mindset that every department within it is a security department (and at the same time an efficiency department). This is the recipe most apt to provide for the secure and efficient movement along the aviation supply chain.

Conclusion

The notion of organizational culture in the provision of aviation security was put forward by ICAO more than a decade ago.[21] But novelty has been hard to come in this area of the air transport industry. Except for behavior observation techniques at a handful of airports, traditional methods of aviation security are still the primary means for security assurance. It must be accepted that these methods shall be the mainstay of aviation security services for the long term. But concerns must be raised about the ability of one-size-fits-all, indiscriminate security screening methods to cope with the relentless growth in demand for air travel. In this context, the imaginable scenario is that there would be serious bottlenecks in the flow of passengers and cargo because airports would be under strain to cater for the increased security footprint as the rate of growth of aviation infrastructure will not be able to match the growth in demand.

Based on the premise that no activity is privileged with access to unlimited resources, the judicious use of such finite resources should therefore be a natural feature of the security process. The use of an adequate dose of intelligence in the detection of security threats will go a long way to alleviate the ever-increasing workload resulting from the relentless growth in demand for air travel and at the same time lower the cost of security provision.

The issue of intelligence inevitably points to the human element and its capability to act proactively and predictively which in turn leads to the notion of advance information (which incidentally is inherent to safety-critical services and has been instrumental in the achievement of the legendary safety record which is the pride of civil aviation). The ability to acquire (and disseminate, after analysis and decision making) advance security data requires specific skills considering the real-time environment of aviation operations and the psychological impact normally associated with security events. It is therefore essential that the policing and enforcement perception that has characterized aviation security for so long integrates an intelligence component that enables a more efficient focus on outcomes (preventing illicit matter getting on board aircraft).

Civil aviation is a mode of transport characterized by the application of global standards but also requires long lead times for its human element to acquire competencies. An international drive is warranted to review the skill requirements of aviation security personnel with focus on intelligence-based detection and a culture that generates trust and collaboration. Only then the viability of an ever-growing and secure aviation supply chain would be assured.

The implementation of novel ways of doing things in aviation can be a daunting task as tradition has prevailed for long. The quote by Andrew Thomas whereby most aviation services are “not much different than 20 or 30 or even 50 years ago”[22] is very pertinent.

[21] ICAO Document 9808 (2002), Chapter 3.

[22] Andrew Thomas: Soft Landing, Airline Industry strategy, Service and Safety, Apress (2011).

New ideas for the provision of aviation services, security included, should not be mere slogans under which tradition thrives, but should be pragmatically implemented and result in tangible benefits. While the genuine global concern for the long-term sustainability of air transport cannot be questioned, bold decisions should be taken to pragmatically achieve it.

References

Airbus Global Market Forecast 2012–2031: navigation the future, p 12 (Executive Summary)
Annex 17 to the Convention on International Civil Aviation, Editions 1 to 9
Ashforth BE, Humphrey RH (1995) Emotion in the workplace: a reappraisal. Hum Relations 48:97. doi:10.1177/001872679504800201
Bisel RS, Messersmith AS, Keyton J (2010) Understanding organizational culture and communication through a gyroscope metaphor. J Manag Educ 34(3):342–366. doi:10.1177/1052562909340879
Boeing world cargo forecast 2012–2013, p 1 (Executive Summary)
Driskill GW, Brenton AL (2011) Organizational culture in action, a cultural analysis workbook, 2nd edn. SAGE Publications, Inc., Los Angeles
Edwards (1972) Human Factors in Aviation. Earl L. Wiener & David C. Nagel (Eds.) (Elsevier, 1988) p 11
Ekman P (2009) Telling lies: clues to deceit in the marketplace, politics and marriage, revised edn. W.W. Norton and Company, Inc., p 349
Goleman D Emotional intelligence, why it can matter more than IQ, Kindle edition. Bloomsbury
Hawkins (1984) ICAO Circular 216, p 7
ICAO Circular 216 (1989) Human factors digest no. 1. Fundamental human factors concepts
ICAO Document 9808 (2002) Human factors in civil aviation security operations, 1st edn
ICAO Document 9859 (2013) Safety management manual, 3rd edn
Keyton J (2011) Communication and organizational culture, a key to understanding work experiences, 2nd edn. SAGE Publications, Inc, California
Kondalkar VS Organizational behaviour. New Age International (P) Limited
Proceedings: 43rd annual 2009 international Carnahan conference on Security Technology (Oct 2009). Institute of Electrical and Electronical Engineers, Zurich
Reason J (2013) A life in error, from little slips to big disasters. Ashgate Publishing Company, Farnham, Surrey, England
Reason J The Swiss Cheese Model
Schein EH (2010) Organizational culture and leadership, 4th edn. John Wiley & Sons, Inc.
Schermerhorn JR Jr, Hunt JG, Osborn RN, Uhl-Bien M. Organizational behavior, 11th edn. John Wiley and Sons, Inc.
Schultz D, Schultz SE (2001) Psychology & work today, 8th edn. Pearson Education, Inc.
Schwaninger A (2009) Why do airport security screeners sometimes fail in covert tests, 43rd ICCST, Zurich
Stolzer AJ, Halford CD, Goglia JJ (2011) Implementing safety management systems in aviation. Ashgate Publishing Company
Stolzer AJ, Halford CD, Goglia JJ (2012) Safety management systems in aviation (Reprinted). Ashgate Publishing Company
Tony Tyler, Director General and CEO, IATA at 21st AVSEC WORLD (IATA Aviation Security Conference), March 2013, Brooklyn, New York (http://www.iata.org/pressroom/speeches/Pages/2013- 03-05-01.aspx)

An Evaluation of Capacity and Inventory Buffers as Mitigation for Catastrophic Supply Chain Disruptions

James R. Bradley

Abstract By some accounts supply chains are increasingly being affected by catastrophic events that disrupt goods flow for prolonged periods. This may be because the occurrence of catastrophic events has, indeed, increased or because we are simply more attuned to such events because global supply chains are exposed to a greater number of catastrophic risks. Regardless of which is true, arguments have been made in the popular press that the impacts of catastrophic events are more severe than in past years because supply chains have less inventory which reduces the amount of time before deliveries to customers are affected. These same accounts argue for managers to return to past practices where more inventory was held, which motivated the analysis in this article of whether such inventory buffers are financially feasible. To broaden the discussion, we also analyzed whether the alternative type of buffer, manufacturing capacity, is feasible. We characterize the feasibility of these two buffer tactics by measuring their effect on manufacturing companies' net incomes and credit worthiness. We also discuss nonfinancial factors that determine whether capacity and inventory buffers are effective as well as provide some ideas for restructuring supply chains so that less capacity is needed to mitigate the effect of catastrophic disruptions.

Keywords Catastrophe • Catastrophic event • Catastrophic supply chain failure • Disaster • Disaster management • Enterprise risk management • Resilient supply chains • Risk • Risk management • Risk mitigation • Supply chain management • Supply chain risk management • Supply chain risk mitigation

Introduction

Perhaps the simplest way to describe the goal of supply chain management is to manage supply so that it matches demand as closely as possible. If raw materials are received and subsequent manufacturing and distribution operations are performed

J.R. Bradley (✉)
Raymond A. Mason School of Business, The College of William and Mary, Williamsburg, VA, USA
e-mail: james.bradley@mason.wm.edu

A.R. Thomas, S. Vaduva (eds.), *Global Supply Chain Security*,
DOI 10.1007/978-1-4939-2178-2_7

in clockwork fashion so that customers receive goods in the precise quantity desired exactly when they are desired, then the needs of the customers and the company are perfectly served with the manufacturer needing to produce no goods in excess of those demanded by customers. The most significant difficulties in achieving that goal perfectly are posed by uncertainty and lead time. Uncertain and varying customer demand forces manufacturers to order and make excess goods just in case demand is greater than expected. Uncertain timing or parts deliveries as well as uncertainty about the quantities that may arrive cause manufacturers to either order early or order quantities exceeding anticipated needs. Uncertain manufacturing output and transportation times also cause goods to be made or shipped earlier than otherwise would be necessary. All these responses to uncertainty cause excess inventory that is called safety stock, which increases with greater uncertainty. Longer delivery and manufacturing lead times also increase safety stock levels because managers need to forecast, or guess, what demand might be in farther into the future, and forecasts farther into the future most often have greater error: more things can "go wrong" over the longer time period. As uncertainty and the time goods take to get through the supply chain increase, safety stock increases.

Managers can also compensate for uncertain manufacturing output and customer demand quantities by having the capability of producing goods at a faster rate. The production rate, for example, in units produced per hour, is often referred to as manufacturing capacity. Demand spikes are accommodated more quickly with some buffer capacity in place, which reduces the need for a safety stock of finished goods. Without extra capacity or extra inventory, it is, of course, the customer who suffers the effect of uncertainty when their deliveries arrive late. Late deliveries, especially if persistently late, cause future sales to be lost. Hopp and Spearman (1996) echo that the cost of variation comes in the form of investment in extra capacity, procurement of extra inventory, or in delayed delivery to customer: one of these variables must yield. Thus, a tradeoff exists among capacity, inventory, and customer service as shown in Fig. 1. Managers must meet uncertainty and increased

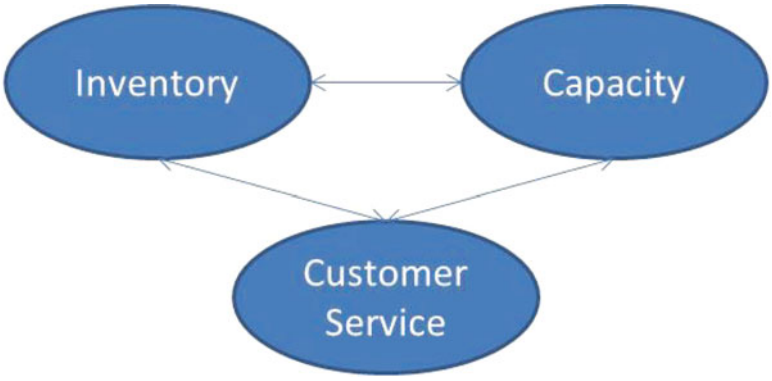


Fig. 1 Capacity, inventory, customer service tradeoff

lead times with some measure of increased inventory, increased capacity, or reduced customer service. The "mix" of capacity and inventory, and the desired level of customer service, varies from company to company and factors such as the relative costs of buffer capacity and inventory versus customer expectations determine appropriate buffer strategies. The nature of goods also influences whether capacity or inventory buffers are best; for example, it is difficult to keep large inventories of perishable goods.

Operations management professionals have become accustomed over the years to a certain level of uncertainty and unpredictable variation in demand levels, equipment downtime, worker absenteeism rates, and supplier delivery performance. Managers adjust to these uncertainties either through adjusting capacity and inventory levels using either rules of thumb that are informed by substantial experience or using formulas developed in academic research. These historic, continual disturbances in supply or demand are mild in comparison to catastrophic disruptions that by some accounts are more prevalent than in the past.

The duration of a supply chain disruption is one gauge of impact, and whereas most disruptions are on the order of minutes or perhaps hours, Bradley (2014) lists disruptions that range up to 3 months in the case of the Fukushima earthquake which disrupted automobile production and delayed the introduction of Apple's iPad2 (Abe and Hoontrakul 2012). Other well-known events that affected many supply chains include:

- Taiwan earthquake (1999)
- 9/11 attack (2001)
- West Coast US dock strike (2002)
- Hurricane Katrina (2005)
- Changes in US apparel import quotas (2005)
- Fukushima earthquake (2011)

Disruptions whose effects are not widespread, yet still catastrophic, include the bankruptcy of suppliers such as when the bankruptcy of UPF-Thompson threatened Land Rover production in 2002 (Christopher and Peck 2004) and a fire that disabled a Philips wafer fab for 6 weeks (Latour 2001), which caused Ericsson to delay introduction of a critical new cell phone model, significantly weakening its competitive position. Long disruptions suggest that substantially greater buffers are required than for mild variation as Lapide (2008) describes:

> Catastrophic disruptions in supply chains are an extreme form of variability and so significant buffers are required to cope with these sorts of variability in comparison to the daily slightly late deliveries, higher than average absenteeism, machine breakdowns and so forth.

Two other characteristics of catastrophic supply chain disruptions are that any particular event that might cause such a disruption is of very small probability, and the possible events are innumerable. An innumerable number of rare events pose multiple problems, one of which is unpredictability. Planning for any one event is unlikely to pay off and a company's limited resources allow mitigation efforts for only a miniscule percentage of the possible disruptions. Some, such as Bradley (2014),

have analyzed robust methods of mitigation rather than focusing on singular events such that mitigation is more comprehensive and cost effective. This approach, as must all approaches, relies on capacity and inventory buffers.

Some have commented that catastrophic supply chain disruptions seem more severe in the current business climate because companies have leaned down inventory levels over the past 30 years (Kachadourian 2001; The Economist 2006; McGillivray 2000). The implication is that returning to the practice of maintaining higher inventory levels would mitigate the effects that managers are increasingly observing due to catastrophic disruptions. These arguments motivated this article and a thoughtful analysis of inventory buffers for catastrophes, as well as the alternative, capacity buffers.

Capacity to produce is made possible most fundamentally by equipment and human resources. Failures of either mechanical or human resources in any supply chain link disrupt capacity and stop the flow of goods toward customers. The effect of such an outage can be mitigated by either having an alternate capacity source or storing capacity in the form of inventory. Designing an inventory buffer requires specifying (i) where in a supply chain the buffer should be created and (ii) how many of each item should be kept in inventory. Both facets affect the cost of inventory as well as the protection it affords, which we later discuss. Fashioning a capacity buffer is more nuanced than is the design of an inventory buffer. Certainly the "where" and "how much" dimensions of the decision are relevant, but a manager also must consider whether buffer capacity should be established in separate companies than existing capacity, whether diversifying the location risk of its own capacity or supplier plants is prudent, the effect of significant investment in dedicated assets, and the risk posed by localities in terms of a sufficient labor supply or a technically skilled one. Despite this complexity and less observable capacity costs, we are able to execute a pro forma financial analysis on capacity buffers as well as inventory buffers.

Our evaluation of the financial feasibility of an inventory buffer strategy in the next section is accomplished by gauging the financial effect of inventory buffers on a company's financial performance using net income and credit worthiness. Buffers need not be composed solely of either inventory or capacity, and our analysis evaluates the financial impact of inventory buffers that range from the stockpiles requires for a buffer exclusively of inventory to one that would require the additional cost of a supplemental capacity buffer: if the inventory portion of a composite buffer is financially infeasible, then that composite buffer remains infeasible when the cost of capacity is added.

In the subsequent section we discuss capacity buffers. A comprehensive evaluation of the feasibility of a capacity hedge is difficult due to the many facets of a capacity buffer and the nontransparent costs of various buffer tactics such as contracting for contingency sourcing or flexibility in order quantities, the loss of economies of scale (or the benefits) due to dual sourcing rather than sole sourcing, and so forth. Product complexity and other part characteristics also affect buffer capacity decisions and process flexibility further exacerbates the problem. We address this difficulty by parameterizing the effects of product complexity, flexibility

of assets, and the intensity of a company's manufacturing assets. In the final section, we conclude by drawing the two discussions of inventory and capacity buffers together.

Inventory as a Buffer Against Catastrophic Disruption

Inventory can be in various states of completion from raw materials at the beginning of a supply chain, to work in process at intermediate links of a supply chain, to finished goods at the end of a supply chain. In this section, we first discuss how the cost and the risk protection offered by an inventory buffer varies depending on it placement in the supply chain. Further we argue for evaluating risk protection in the form of finished goods inventory absent idiosyncratic details of specific supply chains. Subsequently we analyze the financial feasibility of such a buffer and comment on other nonfinancial factors that affect inventory's effectiveness as a buffer.

How Characteristics of Inventory Buffers Vary with Supply Chain Location

It is perhaps fair to say that the most significant effect of catastrophic events is on capacity, whether the capacity is disabled or made inaccessible. If the sole effect of a disturbance is to destroy inventory, then that inventory might be replaced in relatively short order. It might take considerable longer to repair devastated equipment and buildings. It took 6 weeks to repair the Philips Albuquerque despite the fire lasting only 10 min. Earthquakes or tsunamis might require total reconstruction of a plant. No manufacturing capacity was destroyed in the 9/11 attacks but subsequent heightened security checks at US-Canada border made the output of Canadian auto suppliers inaccessible to US assembly plants. It is difficult to think of catastrophic events that affect solely inventory stockpiles and having no effect of production or transportation. Thus, our discussion of inventory frames it as a reservoir of stored capacity that can be used when catastrophe disables capacity, although inventory provides only temporary relief until it is exhausted. Inventory, however, can substitute only for upstream disabled capacity because releasing goods into a downstream obstruction does no good. Inventory buffers that are placed further upstream, therefore, mitigate fewer of a supply chain's capacity resources and, thus, fewer of the many possible catastrophic events. Conversely, as inventory is moved downstream, it provides protection against a greater number of possible disruptions, but its value also increases, as measured by standard accounting practices, because more work has been done on it. For example, inventory valuations on balance sheets and cost of goods sold on income statements include labor costs incurred for processing goods. Figure 2 summarizes this discussion by mapping this risk-cost profile depending on inventory buffer location.

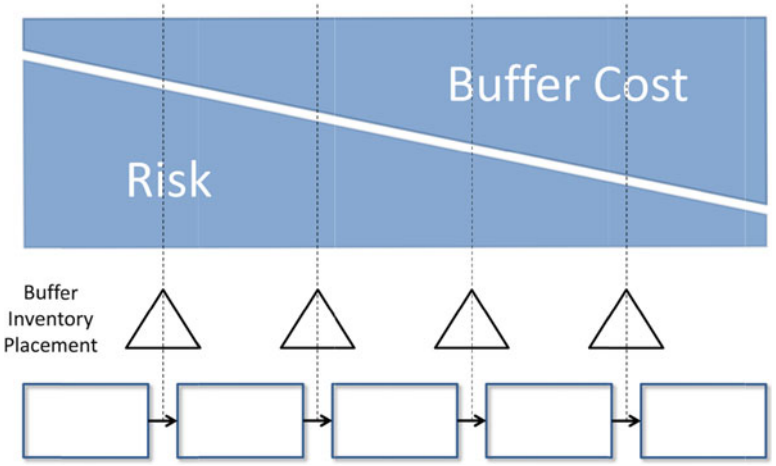


Fig. 2 Risk-cost profile of inventory buffers

Another cost of moving inventory downstream is that it becomes less flexible: as goods are processed they become specialized to fewer and fewer products. For example, iron ore can be used in any type of steel or cast iron. Once made into steel and the carbon content and alloy determined, it can be used in many fewer circumstances. Once rolled, its use is still more specific to instances where its thickness is appropriate. Once stamped into a part, it can be used on only one model of car or appliance. Goods stored earlier on in a supply chain in more flexible forms, therefore, allow inventory buffers to be smaller and less costly. This popular notion of holding goods as far upstream as possible is often called form postponement and it exploits the technical concept of risk pooling. In distribution, where the form of goods are not changed, but their locations are, the analogous notion of location postponement applies: goods held farther upstream are more economically distributed to a greater number of downstream locations. Inventories cannot be held so far upstream, however, such that the supply chain becomes unresponsive. The additional inventory buffer required to provide a certain level of customer service increases in proportion to the square root of the number of distinctive product variants at the link of the supply chain where the buffer is placed.

The optimal location of buffer inventory to negotiate this tradeoff varies from industry to industry and company to company. However, if the dominant criterion is risk reduction, then downstream buffers are best, which is why we analyze a buffer of finished goods inventory at the end of its supply chain. Note that a finished goods inventory is not a perfect buffer for catastrophe. This inventory, too, can be wiped out by a catastrophic event or made inaccessible due to infrastructure damage (damage to utilities, roads, etc.). We will ignore these possibilities and assume that inventory is always accessible and unharmed. On this dimension our evaluation of inventory as an effective buffer is optimistic.

Note that our analysis of inventory buffers is relevant only to manufacturing processes that produce physical goods because inventory buffers are impossible in service and administrative processes where work cannot be processed in advance due to the unique nature of each request: only capacity buffers are possible in these environments. This comment also applies to make-to-order manufacturing. Dell, for example, makes computers to order for its online consumers and a core feature of its business model is delaying final assembly until orders are received and delaying ownership of raw material as long as possible.

Inventory Buffer Evaluation Methodology

Tomlin (2006) compared the use of inventory buffers with buffer capacity in the form of a second supplier using a theoretical optimization model of what can be construed as a two links of a portion of a company's supply chain processes. He found that providing protection against disruptions with inventory is tenable for short, frequent disruptions but not for long, rare disruptions. While our analysis is perhaps simpler, it is done in a way that comprehends all the supply chains in which a company participates and assesses not "which alternative is better" but rather what buffer tactics are feasible in view of an entire firm's operations vis-à-vis its income statement. Tomlin's study has its advantages, but it can only say which is a better strategy for a microcosm of a company's operations but not whether either is feasible financially. If a buffer against catastrophe is not financially viable, then it cannot be considered even if it is the best of the alternatives considered. A buffer intended to possibly provide protection in the long term is counterproductive if it drives a company into bankruptcy in the short term.

We evaluate the financial effects of implementing an inventory buffer by considering whether a company remains profitable with the cost of the buffer factored in and by assessing the secondary effects of financing an inventory buffer. The metric we will use for profitability is net income. Regarding the latter criterion, the change in financial structure to implement an inventory buffer could cause banks and the debt markets to view the company as being a greater credit risk, which would increase the interest rates on bank loans and increase coupon payment rates for new debt issues. Banks, in the worst case, could call lines of credit and other financing instruments if financing inventory caused companies either to violate covenants or to be unable to meet their cash flow requirements including debt service. While we cannot predict exactly the financial effects of having a "riskier" financial structure, we can gauge whether credit sources would be likely to take some or all of the previously mentioned actions. To this end we will use a metric that is widely used to evaluate debt worthiness, which is funds flow coverage (FFC):

$$\text{Funds flow coverage} = \frac{\text{EBIT} + \text{depreciation}}{\text{Interest expense} + \dfrac{\text{Debt repayment}}{1 - \text{tax rate}} + \dfrac{\text{Preferred dividends}}{1 - \text{tax rate}}},$$

Table 1 Inventory carrying cost components

Cost component	Annual % carrying cost	
	Minimum	Maximum
Cost of money	6	12
Taxes	2	6
Insurance	1	3
Warehouse expense	2	5
Physical handling cost	2	5
Clerical and inventory control	3	6
Obsolescence	6	12
Deterioration and pilferage	3	6
Total	25	55

where EBIT is earnings before interest and taxes (Palepu and Healy 2013). FFC measures the extent to which cash flow before interest and taxes and depreciation (in the numerator) can satisfy the certain costs of financing a company's debt (in the denominator). A "cushion" exists for reinvestment in the company and for paying dividends to common shareholders to the extent that FFC exceeds 1. The inclusion of preferred dividends in the denominator reflects the assumption that disappointed preferred investors' would significantly and negatively impact the market's view of the company. A value less than 1 indicates that a company cannot meet its instant obligations and is drawing down equity in the firm: bankruptcy occurs when an FFC of less than 1 persists for a sufficiently long period. An FFC value close to one or less than one would cause financiers to pull their support or increase interest rates, thus further reducing a company's financial standing from the effects of implementing an inventory buffer.

A company's investment in inventory appears as an asset on the balance sheet and impacts the income statement through various types of carrying costs. Richardson (1995) estimated the annual carrying cost for each type of inventory carrying cost as a percentage of inventory value (see Table 1). While other costs might be added to those from Richardson, these components serve as a conservative (low) estimate. We will use Richardson's guidance for all cost components except for the "cost of money" because our data allows for company-specific estimates of this cost of financing.

The numerator of FFC is reduced by all the cost components in Table 1 except the cost of money because interest is not included in EBIT. The additional financing cost does increase the denominator. Assumptions about how inventory is financed, whether financing be short term or long term, determine how financing an inventory buffer affects the debt repayment term in the denominator of FFC. With long-term financing, debt repayment would be required to reduce the debt principal, which would reduce FFC through vis-à-vis a larger debt repayment term in the denominator. Short-term financing would require the financing to be continually refreshed so that interest would be continually incurred, but there would be no debt repayment. It is not clear how any company would finance inventory. While inventory is listed on balance sheets as a current asset and the well-known matching principle in finance suggests that current assets should be financed with short-term financing, the perpetual nature of a large inventory buffer might motivate long-term financing.

We evaluated the financial effectiveness of inventory protection using the Compustat database from the Wharton Research Data Services (WRDS) for companies registered as doing business in manufacturing as represented by NAICS codes starting with 31 through 33, which encompassed 1,748 companies for the fiscal year 2013. Financial statements in that database did not enable separate computations for both short- and long-term borrowing and bond debt, although an overall interest rate for both long- and short-term borrowing combined was possible. We used that combined rate which we estimated by dividing interest and related expense (which includes bond coupon payments) by the sum of long- and short-term debt. We, then, added that financing rate to the other carrying cost components from Richardson to arrive at an overall carrying cost that we applied to the additional buffer inventory. Such an estimate could not be computed for 549 of the companies because either there was neither long- nor short-term debt or interest expense was zero. In this case, we made an optimistic assumption that financial carrying cost was at the risk-free rate. No method for estimating the risk-free rate is uniformly accepted although the return for short-term government bonds is a common proxy. Accordingly, we used current rate of return for 1-year government bonds, which is 0.10 % per year as of this writing. We assumed that all financing of additional inventory was short term so that debt repayment in FFC remained unchanged from the year last reported: this also creates an optimistic estimate of FFC whereas any long-term financing would increase debt repayment while decreasing FFC.

We evaluated finished goods inventory buffers from 0 weeks to 52 weeks of protection commensurate with the potential long-term disruptions of supply chains. The Compustat database distinguishes among inventory types and so most often the current level of finished goods inventory is often specified: in other cases it can be reasonably estimated. Our analysis accounted for inventories already in place: no additional buffer was imputed into a company's financial structure if the duration being evaluated was less than the existing FGI protection although these buffers might not be structured for the purposes of risk mitigation.

Cost of Goods Sold (COGS) from the income statement divided by 52 was used to judge the average value of finished goods needed to cover 1 week of demand. Of the 1,748 companies 116 were excluded from the study because no COGS was reported which prevented computing the appropriate inventory buffer size. In addition, when companies had no debt, no interest charges, no preferred dividends, and existing finished goods inventory in excess of the protection duration being tested, they could not be included in the FFC analysis because the denominator of FFC would be zero. Many companies affected by this requirement tended to be in the pharmaceutical industry, which may be involved in research and development but actually produce no physical goods. Other companies in this group might be start-ups with alternative financing. This caused the basis number of companies to change depending on the protection level being tested so that the percentages of companies with substandard FFC performance do not always monotonically increase as the protection level increases.

While estimates of the cost of money were possible for the companies via financial statements, the other carrying cost components are more difficult to ascertain for specific companies. Thus, we evaluated over a range of possibilities

including the minimum and maximum levels identified by Richardson, as well as the midpoint levels, which are 19, 31, and 43 % excluding the cost of money. To those percentages we added the financing rate for each company as computed from data in the Compustat database. We should not expect inventory carrying cost rates, borrowing, and expenses to be insensitive to an increasing inventory buffer. For example, significant increases in inventory levels would require new construction and the concomitant investments or access to additional floor space via third party logistics providers. Our analysis is, again, optimistic regarding an inventory buffer in ignoring these detrimental effects of large inventory investments.

Results

The results were relatively insensitive to inventory carrying costs excluding the cost of money, and so we report the results for the midpoint carrying cost as a representative scenario. Table 2 shows the percentage of companies with unsatisfactory FFC (<1) and negative net income as the inventory buffer protection duration increases from 0 to 52 weeks. We observed that a significant number of companies are not financially sound in their existing state: 739 companies currently have an FFC less than 1 and 706 companies have negative net income. As inventory or capacity buffers were added, the number of firms with substandard financial performance increased from these bases.

We previously mentioned disruptions of durations up to 12 weeks (Fukushima). For this disruption duration, the commensurate inventory buffer would cause 64.4 % of companies to have negative net income and 61.0 % to suffer secondary financing effects.

Table 2 Effect of inventory buffer on pro forma financial performance

	FFC		Net income		
Inv. buffer (weeks)	# of companies with FFC < 1	% of companies with FFC < 1	# of companies with net income < 0	% of companies net income < 0	% net income decrease for profitable companies
1	816	55.1	819	55.3	0.7
2	823	54.9	827	55.2	1.7
3	834	55.3	830	55.0	3.9
4	846	55.7	842	55.4	6.4
5	858	56.1	856	55.9	9.1
10	931	59.1	974	61.8	21.8
12	970	61.0	1,024	64.4	26.1
15	1,012	63.1	1,105	68.9	30.0
20	1,094	67.9	1,212	75.2	36.6
26	1,158	71.5	1,324	81.7	41.9
30	1,198	73.9	1,381	85.1	44.4
40	1,301	80.6	1,485	91.3	46.1
52	1,387	85.2	1,545	94.9	49.2

For longer disruptions, say the maximum duration tested, 52 weeks, 94.9 % of companies would have negative net income and 85.2 % would suffer secondary financing effects. Financing inventories to withstand extremely long disruptions, thus, seems implausible for a majority of companies. In addition, we computed the percentage reduction in net income for companies that remained profitable with inventory buffers, as shown in Table 2. While these companies remained profitable, the decrease in net income for larger inventories was substantial, approaching 50 %, which would be a significant consideration in evaluating the feasibility of large inventory buffers. This financial observation will be considered in the final section together with operational considerations that compound the problem of large inventories, as well as the analysis of capacity in the next section.

Capacity Buffers Against Catastrophic Disruptions

General Considerations for Buffer Capacity

Capacity resides at all links of a supply chain, within a focal company (unless all manufacturing is outsourced) and at all previous stages of supply. In determining how a capacity buffer might be implemented, one must determine where in the supply chain buffer capacity would be placed. To the degree that companies rely on suppliers to self-protect against catastrophic failure, then the financial impact of supplier's buffers is manifest in some combination of increased unit costs for the buyers and reduced profits for the suppliers. Companies sometimes require suppliers to have business continuity plans to ensure this protection is in place. Even with supplier self-protection, a company might have alternate sourcing available for additional protection since no operation can be rendered 100 % reliable. A company can back up its own capacity by maintaining the buffer itself or by having a supplier who is able to perform the same operations. In determining the cost of a capacity buffer, we, therefore, need to consider the scope of the supply chain to be protected and the entity that will maintain the buffer. Supplier contracts are private and so it is difficult to ascertain what unit cost premium (or discount) a company might incur, for example, for splitting supply between two suppliers or arranging for idle, reserve capacity at a backup supplier.

Bradley (2014) lists categories for catastrophic disruptions. Of those categories, the following risk categories, or failure modes, are those that are affected by a company's decision about how many suppliers to maintain and which ones to use:

- Part supply failure
  - Process failure (machinery failure, people skills shortage, calibration, etc.).
  - Specialized vs. commodity parts affect time required to bring new source online.
  - Supplier market with few possible suppliers affects recovery time.

- Supplier failure
  - Bankruptcy
- Facility failure
  - People resources shortage.
  - Worker-management relationship failure.
  - Quality management affects probability of catastrophic quality failure.
  - Facility construction affects propensity for catastrophic damage.
- Location disruption
  - Disrupted infrastructure inhibits access to supply within region.

These failure modes suggest that putting buffer capacity in place is not simply a matter of expanding current capacity. Unless buffer capacity is placed in a different organization, the risk of losing all capacity due to bankruptcy remains unchanged. Unless the buffer capacity is in a different location, it is vulnerable to the same local disruptions. Finally, if located in the same facility as other parts production, all these parts are vulnerable to the same facility failures. Mitigating the attractiveness of reducing risk by maintaining capacity at multiple suppliers, facilities, and locations is the possibility of increased costs due to loss of scale economies. Further, capacity buffer strategies must specify whether the viability of the capacity is to be ensured by using it on an ongoing basis or keeping it idle and in reserve with the possible disadvantage of uncertain readiness.

The amount of capacity employed as a buffer might be that which provides 100 % capacity backup regardless of what event might occur and an undisrupted revenue stream. Partial capacity buffers provide for maintaining a portion of revenues or an uninterrupted revenue stream where the capacity backup fortuitously could replace the manufacturing infrastructure that was disabled. Besides relying on good fortune, the effectiveness of a partial backup in supporting manufacturing on a widespread basis can be planned for using flexible machinery and people who can operate many processes: when similar capacities are scattered in multiple installations each being capable of producing all parts, then a partial increment of capacity at each location can provide an effective backup through the reallocation of production assignments. This, however, seems a more likely strategy for larger companies where production scale affords multiple plants of an economic size.

Capacity Buffer Evaluation Methodology

Since we cannot observe the effects of contracting decisions, we will make an approximate, optimistic analysis by assuming that a company simply replicates some portion of its own manufacturing capacity base and relies on its suppliers to protect their own portions of the supply chain with the possible financial effect of increased unit purchase prices. Balance sheet assets include property, plant, and

equipment (PPE) which are broken down into several components. The relevant components for our analysis are the subcategories of machinery and equipment at cost, buildings at cost, and land and improvements at cost. We assume that the first category is predominantly manufacturing-related equipment that provides capacity. Having the percentage of manufacturing resources in PPE specified for machinery and equipment allows us to control for companies with varying degrees of outsourcing such as Apple and Cisco Systems, which have little or no manufacturing, to companies that maintain significant manufacturing capabilities. The last two components include manufacturing-related assets as well as other assets related to administrative functions. The portion of these assets that are related to manufacturing will vary depending on outsourcing policies and how many separate facilities are used for headquarters and other offices for research, marketing, and other non-manufacturing functions. Accordingly, we attribute only a portion of these two asset components to manufacturing capacity. Some companies are devoid of manufacturing facilities, and this portion may be close to zero, while the percentage could be large for other companies with modest headquarters. Thus, we test a range of percentages, from 0 to 100 %.

We discussed the possibility of a partial capacity backup providing for full maintenance of a review stream through production flexibility, particularly for large companies. We will subsume these effects into a factor we call "flexibility and scale." The larger and more flexible a firm, the greater might its opportunities be to protect itself with a smaller percentage of incremental capacity buffer. We will test percentages from zero percent to 100 % in increments of 10 %: 0 % would be representative of a company that was large and had sufficient flexibility or already maintained a sufficient buffer, while 100 % would be appropriate for inflexible manufacturing processes with little existing buffer. While we cannot know which percentage precisely fits with any company, we can measure how many companies could withstand capacity additions at various points in this range.

Added to the borrowing required for fixed investments in capacity and the related interest or coupon payment expense are maintenance costs, which would be incurred even for machinery that is idle and held in reserve. Maintenance costs of manufacturing equipment, however, are difficult to tease out precisely from the operations expense line on income statements. The percentage of operating expenses that are due to maintenance would obviously vary from company to company, and we use 5 % of the equipment value as a rough estimate of annual maintenance costs based on operations with which we are familiar: this will be high for some companies and low for others. Our analysis essentially assumes either that the additional capacity is not operated but held in reserve or, equivalently, that no economies are lost by separating manufacturing capacities. Otherwise, we would need to increase labor costs.

As was done in the analysis of buffer inventory, we judge the efficacy of a capacity buffer using net income and FFC. It is assumed that all additional equipment would be financed with long-term borrowing using the matching principal. Depreciation is an added income statement item that increases with additional equipment purchase, but the useful lives of equipment and depreciation schedules vary by industry and with the type of equipment. We approximate each company's

depreciation rate by dividing its current annual depreciation by total PPE. Accelerated depreciation schedules imply that this estimate is sensitive to how the ages of existing equipment are distributed, and so the implicit assumption is that current depreciation is representative of the portfolio of equipment in use in any given year. Debt repayment on the new long-term financing is calculated on the basis of repaying the debt in 10 years commensurate with the economic life of many assets.

For analysis of net income, we could estimate a depreciation rate when companies reported PPE and depreciation, which allowed the analysis for 1,541 of the 1,748 companies. Additional exclusions were necessary for our analysis of FFC when neither debt nor interest expenses were reported which makes the FFC denominator zero, which left 1,316 companies in the analysis.

Results

We observed that the pro forma financial health with added capacity buffers as measured by net income and FFC is relatively insensitive to the percentage of PPE associated with manufacturing capacity for non-equipment PPE. Therefore, we will report data for an intermediate percentage of 50 %. Of the companies amenable to this analysis, 680 had current net income less than zero and 706 had a current FFC < 1.

Table 3 shows that a majority of companies cannot support even a modest capacity buffer financially: even a 10 % buffer capacity is infeasible for most companies. While that is true, one also can observe that a capacity buffer is feasible for a greater percentage of companies than is a substantially sized inventory buffer: 100 %

Table 3 Effect capacity buffer on pro forma financial performance

	FFC		Net income		
"Flexibility/ scale" % incremental capacity buffer	# of companies with FFC < 1	% of companies with FFC < 1	# of companies with negative net income	% of companies with negative net income	% net income decrease for profitable companies
0	706	53.6	680	44.1	0.0
10	788	59.9	797	51.7	3.8
20	814	61.9	821	53.3	5.8
30	834	63.4	859	55.7	7.1
40	859	65.3	887	57.6	8.4
50	886	67.3	923	59.9	9.2
60	902	68.5	952	61.8	9.9
70	917	69.7	987	64.0	10.2
80	931	70.7	1,011	65.6	10.8
90	945	71.8	1,037	67.3	11.3
100	964	73.3	1,063	69.0	11.6

replication of capacity is feasible for roughly the same percentage of companies as is a 20-week inventory buffer. Table 3 also shows that capacity buffers have a less significant effect on net income than do inventory buffers for companies that remain profitable. Also important to note is that managers can structure supply chains so that less of a capacity buffer would be required by designing products, processes, equipment, and tooling to be more flexible. This flexibility would also have benefit on an ongoing basis for daily non-catastrophic variations in demand and production processes. Examples of designing for flexibility are idiosyncratic to particular production environments, but some examples include these:

- Using the same stamping presses at all plants and commonizing die design so that all dies would fit into all presses
- Using the same material feeding devices in all plants on "chip shooters" in circuit board assembly lines so that material can be moved from one plant to another if needed
- Commonizing geometry of locating holes in automobile floor pans among car models so that they can be processed in all plants
- An increased inventory would also help mitigate demand spikes, although much of a 26-week supply, for example, would remain unused without any ongoing incremental benefit.

Further study is required to determine why more companies can support capacity buffers than inventory buffers and to determine the common characteristics of companies that can support a capacity buffer financially. A first, obvious, hypothesis for the latter point is that companies with few manufacturing assets can successfully finance incremental additions to the few assets they do operate. A cursory overview of the data, indeed, suggests that some companies that are classified by NAICS codes to be "manufacturers," but who have outsourced most or all production, are among the companies whose net income and FFC remain favorable with the addition of a capacity buffer.

Discussion and Conclusions

The pro forma analysis of capacity and inventory buffers showed that while more companies can withstand a capacity buffer financially, neither a capacity nor an inventory buffer of significant size is feasible for a majority of firms. In this section we discuss this result in light of three issues and observations:

1. Additional, nonfinancial factors that further inhibit the feasibility of inventory and capacity buffers
2. Articles in the popular press imply that inventories are effective protection against catastrophic failures
3. The need for innovative tactics to protect against catastrophic disruptions

Our financially oriented analysis ignores many factors that make large inventories costly or ineffective in time of disaster. Inventories that are subject to perishability

make large inventories infeasible because they would continually need to be discarded and replaced. Perishability, in a general sense, encompasses more situations than when foodstuffs spoil. For example, fashion items and other goods with short life cycles can have notoriously high variability in demand, and throwing away or selling at a loss leftover goods at the end of life cycles would constitute a large economic loss. Also, large inventories of goods that are subject to engineering changes could incur substantial costs to either rework or dispose of when specifications change. Further, while it might seem pedestrian to maintain inventories, undisciplined practices often make inventory subject to loss, damage, theft, as well as being difficult to locate in time of need. Finally, among other considerations, buffer inventories must be thoughtfully situated in a supply chain so that they are neither destroyed nor made inaccessible by a catastrophe although the location and characteristics of the next catastrophe are unpredictable.

Buffer capacity implemented with redundant production capabilities in separate facilities or suppliers also has downsides. One notable one is that this practice violates one of the tenets of the Toyota Production System that having all goods flow through the same process minimizes variation in dimensions and other attributes, which maximizes quality (Spear and Bowen 1999). Economies of scale might also be lost in some circumstances

Recent popular articles compare favorably the larger inventories held by companies in past years relative to the current leaner inventories and, either explicitly or implicitly, suggest increased inventories would be welcomed protection against catastrophic disruption. Our analysis would, however, suggest that this is imprudent for most companies from the standpoint of financial feasibility even without considering what potential, eventual return might come from such an investment. It should also be noted that inventory is an effective buffer only if it makes parts available in the appropriate proportions as specified by the bill of materials for the desired finished goods and that inventories are indeed accessible during a catastrophe. Missing any one part prevents goods from being manufactured. A careful analysis of how inventories were held in decades past might show they were held in ineffective proportions and locations, perhaps more haphazard than in a planned manner as is required for disruption protection.

The financial infeasibility of an unimaginative duplication of capacity or bolstering of inventories suggests that risk mitigation needs to be provided in innovative ways for the many companies that cannot afford such investment. Even for those that can an innovative approach, as we discuss in the remainder of these conclusions, is beneficial.

One idea is to establish buffers where they do the most good and are the best alternative. Factors that guide these decisions include the availability of alternative suppliers, whether parts are commodities or highly engineered, part life cycles, and whether tooling is asset specific. These factors influence where the best mitigation tactic would fall on this continuum:

- No capacity backup: react when catastrophe occurs.
- No capacity backup and bridge inventory: use bridge inventory to sustain while new capacity is brought online.

- Capacity backup held idle in reserve.
- Capacity backup used for regular supply; total capacity meets demand.
- Capacity backup used for regular supply and total possible capacity exceeds current demand.

Tactics toward the top of the list are more appropriate when many possible suppliers exist and goods are commodities with well-known specifications. In this case, changing a supplier takes the least time. When parts are more complex or the supplier base less robust, then having a bridge inventory in recognition of the greater duration required to bring another supplier online might be prudent. Capacity (machinery and tooling) might be necessary when it would take a long time to reconstruct tooling that was destroyed or made inaccessible or where specialty equipment is required. Unfortunately, in these cases jigs and fixtures are sometimes asset specific, which means they can be used only for specific parts needed by a specific buyer. For example, if a supplier owns stamping dies that are used to stamp a Ford Taurus hood, then that tooling provides the supplier with no value in making parts for any car company besides Ford. Specific assets are sometimes owned by the supplier and sometimes by the buyer. Regardless of ownership specific assets can become unavailable to the buyer if a disruption were to occur. Creating multiple sets of this type of tooling can increase capacity investment substantially; so while this type of capacity backup might be desired, it can also be expensive.

A tactic for catastrophe mitigation sometimes suggested is to provide buffers of critical parts. The term "critical" here can be viewed many ways. If one considers the bill of materials and assumes that the flow of finished goods should not be disrupted, then all parts are critical. If business strategy dictates that short supply of some finished goods is appropriate in time of disaster, then critical parts can connote providing protection for "flagship" products, or products that are most profitable, or products for its most important customers. The framework above implies a different definition of "critical" which is the duration required to reestablish parts flow under the assumption that a company desires to keep all its products available to customers.

Having flexible manufacturing facilities also can mitigate risk. Particularly if a company or supplier has a number of factories making the same type of products, providing each factory with a modicum of extra capacity and the flexibility to make the products made at *some* of the other facilities allows production to be moved around so that operational factories take up the slack for the disrupted ones(s). Graves and Tomlin (2003) have shown that a small amount of this product mix flexibility can create nearly the same flexibility as if all factories could make all products. While this tactic may be effective only for companies with sufficient scale to have many plants with similar manufacturing processes, it does allow for risk mitigation with possibly much less than 100 % capacity redundancy. That said, some types of flexible tooling are more expensive than dedicated tooling.

A notion allied with a company making its own capacity flexible is creating flexibility in a supplier base. Richardson observes that Toyota maintains multiple suppliers for a particular family of parts and production volumes assigned to each

supplier are adjusted to reward suppliers with good performance and punish those who perform poorly (Richardson 1993). The occasional migration of business among suppliers implies multiple suppliers with similar manufacturing capabilities and suggests that production might also be moved from one supplier to another in case of catastrophe, providing asset-specific tooling was available. This tactic, again, is possible only for larger companies whose supply base includes multiple "substitute" suppliers. Such scale also prevents loss of economies due to splitting a low volume of production among suppliers.

References

Abe S, Hoontrakul P (2012) Fragile supply chains challenged by natural disasters. The Nation, 21 June 2012. http://www.nationmultimedia.com/business/Fragile-supply-chains-challenged-by-natural-disast-30184665.html. Accessed 19 Apr 2013

Bradley JR (2014) An improved method for managing catastrophic supply chain disruptions. Business Horizons July-August 2014, 57(4):483–495

Christopher M, Peck H (2004) The five principles of supply chain resilience. Logist Eur 12(1): 16–21

Graves SC, Tomlin B (2003) Process flexibility in supply chains. Manag Sci 49(7):907–919

Hopp WJ, Spearman ML (1996) Factory physics, 3rd edn. Irwin, Chicago

Kachadourian G (2001) Shutdowns likely to continue. Automotive News 75(5948):1

Lapide L (2008) How buffers can mitigate risk. Supply Chain Management Review 12(4):6

Latour A (2001) Trial by fire: a blaze in Albuquerque sets off major crisis for cell-phone giants – Nokia handles supply shock with aplomb as Ericsson of Sweden gets burned – was sisu the difference? The Wall Street Journal, 29 Jan 2001

McGillivray G (2000) Commercial risk under JIT. Canadian Underwriter 67(1):26–30

Palepu KG, Healy PM (2013) Business analysis & valuation: using financial statements, 5th edn. South-Western Cengage Learning, Mason

Richardson J (1993) Parallel sourcing and supplier performance in the Japanese automobile industry. Strateg Manag J 14(5):339–350

Richardson H (1995) Control your costs—then cut them. Transportation Distribution 36(12): 94–96

Spear S, Bowen HK (1999) Decoding the DNA of the Toyota production system. Harvard Business Review 77(5):96–106

The Economist (2006) When the chain breaks 379(8482). http://www.economist.com/node/7032258. Accessed 8 May 2014

Tomlin B (2006) On the value of mitigation and contingency: strategies for Managing supply chain disruption risks. Manag Sci 52(5):639–657

Closing the Last 1/2 Mile of Emergency Response

Charlotte Franklin and Kiersten Todt

Abstract Information in this paper is the result of recommendations and remedies developed at 'Local Supply Chain Capacity in a Crisis Summit Exercise' held in Arlington, VA 2013 on 30th–31st January, 2013, At the event, which was funded through the Regional Catastrophic Preparedness Grant Program, national private sector and not-for-profit essential resource provider experts in sectors, transportation, communication systems, energy/power, financial resources, medical supplies and other vital supplies, together with emergency managers, discussed best practices and major challenges and exchanged remedy recommendations. The co-authors Charlotte Franklin and Kiersten Todt have worked together in Northern Virginia on projects to develop and shift recovery resource planning models and thinking.

Keywords Resiliency • Recovery resources • Disaster • Community • Supply chain

Introduction

When a disaster of any magnitude strikes, immediate delivery of recovery resources is critical: it saves lives and shortens recovery time. The traditional government-centric approach to emergency resource planning has an inherent weakness: it mostly focuses on disaster recovery resource management mostly after the event. People either wait to see what is needed and then worry about getting the resources in or try to predict what 'might' be needed and where to warehouse and stockpile it. This static planning model is being used for very unpredictable events.

C. Franklin (✉)
Arlington Office of Emergency Management, Arlington, VA, USA
e-mail: Cfrank@arlingtonva.us

K. Todt
Liberty Group Ventures LLC, Arlington, VA, USA

A.R. Thomas, S. Vaduva (eds.), *Global Supply Chain Security*,
DOI 10.1007/978-1-4939-2178-2_8

A solution evolves by opening up a valuable dialogue in pursuit of remedies to supply chain challenges in the delivery of humanitarian aid, pre-event, through greater collaboration with the private sector, using already existing distribution hubs in the community and understanding how supply chains operate in both normal and large-scale events, and through better real-time communication tools. What is the best approach to managing a large-scale event? Admiral Thad Allen (retired), keynote speaker at the 'Local Supply Chain Capacity in a Crisis Summit Exercise' Arlington, VA, January, 2013, explained that he identified a distinction between incident command and theatre command during his experience with the Deep Water Horizon oil spill. Theatre command could be defined as a comprehensive integration of all elements in the region of a disaster during the response and recovery phases.

Theatre command is the approach taken by resilient communities; supply chain resiliency is a critical component of theatre command. A theatre is a combination of incidents and incident personnel under a single incident management organisation. Theatre command not only applies to the location of the incident but also can include the entirety of the air, land and sea area that is or that may potentially become involved in the operation – creates unity of effort. A theatre command approach supports the complexities of what people have to manage in a crisis. Approaching managing an incident as a 'theatre' allows for flexibility in incident management by centralising the command, administrative and support functions while decentralising field operations. Large-scale events go beyond what can be imagined and dealt with locally.

Supply chain resiliency is a critical component of theatre command, which is why this distinction is so important when discussing local supply chain capacity in a crisis. Responsiveness means accurately anticipating demand changes. In a natural disaster, demand shifts unpredictably. Time to react is razor-thin and establishing a single point of demand, instead of forecasting from several sources, can increase demand visibility. Time is not wasted reconciling information from different divisions. Company supply chains respond quickly, scheduling necessary labour resources based on expected volume increases and planning for asset replenishment.

For crisis management, community and regional planning to be effective, the static model of the plans and related documents that are produced must be re-examined and commit to producing dynamic models. Dynamic models are capable of shifting and evolving as resources and needs are available and they adapt to the changing nature of a crisis. It must be ensured that these models use supply chains as the foundation.

Supply chains are designed to adapt to the changes in supply and demand on a daily basis. Because this system, which responds to daily dynamic changes, is the primary infrastructure that carries resources to communities, it is only logical that it would be used as a model for unpredictable events.

Supply Chain Security

According to the Regional Catastrophic Preparedness Grant Program:

> a catastrophe cascades across time and space. A catastrophe is a disaster that spills over previously experienced boundaries and seems to keep spilling. The longer and wider the spill, the less likely there will be a return to anything like the prior, physical, economic, social equilibrium.[1]

Why concentrate on supply chain resiliency? Resolving issues of supply chain resilience and private-sector collaboration pre-event by developing systems and methods to support survivors of a catastrophic event: 'will lessen its effects and even perhaps keep a disaster from becoming a catastrophic event'.[2]

> Catastrophic threats…will seriously compromise or even destroy local capacity or the immediate ability to receive and distribute supplies to consumers. But even where the supply chain's local capability has been obliterated, a catastrophe may be avoided IF the supply chain's capability has survived.
>
> If the ability to source, transport, and deliver supplies persists, local capacity can be re-established in one form or another. But if this strategic capacity has also been destroyed – or for some reason cannot be deployed – then a catastrophe is nearly inevitable.
>
> If supply chains are resilient, catastrophe is less likely. If supply chains fail, catastrophe is much more likely.

The biggest challenge around recovery resource management is that everything that has been done up to now has not fully addressed these issues. Although emergencies, by their very nature, are unpredictable events – which is contradictory to the concept of pre-event planning – can a community affect the degree of physical, economical and psychological damage they may cause and, if so, how? In order to further investigate remedies that might mitigate a disaster's effect on the community, it is better to first understand what happens in the supply chain when 'normal' abruptly shifts to 'emergency'.

[1] Regional Catastrophic Preparedness Grant Program (RCPGP) (2012).

[2] FEMA (2012).

What Changes?[3]

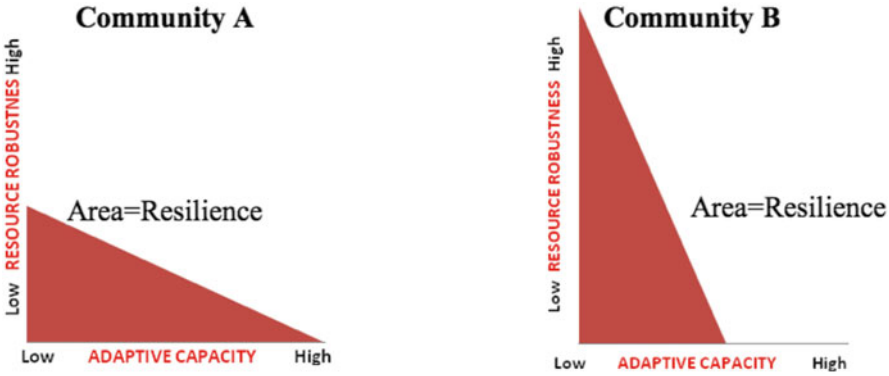
Characteristic	Commercial logistics (normal)	Humanitarian logistics (emergency)
Objective pursued	Minimisation of total logistic costs	Minimisation of human suffering
Commodity flows origination	Self-contained	Affected by material convergence
Knowledge of demand	Known with some certainty	Unknown and dynamic due to lack of information and access to the site
Decision-making structure	Structured interactions under control of a few decision makers	Nonstructures interactions with influences of possibly hundreds of decision makers
Periodicity/volume of logistic activities	Repetitive, relative steady flows, 'large' volumes	Once in a lifetime events, large pulse of flow, relatively 'small' volumes
Supporting systems (e.g. transportation)	Stable and functional	Affected and dynamically changed

Is it really possible to have rigid plans with predetermined resource inventories in place for all possibilities, when what will happen in unpredictable? Are there ways to ensure one's own redundancies? Are there solutions to accessibility, security and credentialing? Are the correct prioritisations in place? Can implementation recommendations be developed for communication gaps? Because these recurring challenges are predictable, can local government and the private sector collaborate to develop flexible alternative 'workarounds' and establish communications plans to be activated in post-disaster recovery?

To be resilient, a community must have both the resources available and the ability to apply or reorganise them in such a way to ensure essential functionality *during* and/or *after* the disturbance. Communities with a highly robust pool of resources and a high degree of adaptive capacity will be the most resilient. Communities that possess low levels of resources *and* low levels of adaptive capacity will be less resilient. If a community is lacking in resources, it should concentrate on building flexibility to be more adaptive.

[3] Holguín-Veras et al. (2012).

Resource Robustness and Adaptive Capacity[4]



An examination of these issues reveals challenge areas and remedies for how one might mitigate the impact that an event could have on recovery by using a more flexible 'supply chain' model that can adapt more readily to supply and demand shifts that occur when disaster strikes. These challenges can be addressed in isolation of each other, by examining them by sector and supply chain delivery needs, in order to understand their impact and effects; the interdependencies are reflected in the remedies. Selected sectors and their challenges are outlined below.

Infrastructure Challenges

Transportation

The USA has a huge intermodal transportation system and the reality of this complex system is that it faces great challenges in its continued growth and its ability to enhance efficiency because it has grown by mode more forcefully than through intermodal growth. Today's national arguments often focus on mode versus mode, such as the rail industry objecting to longer and heavier trucks on interstate roads.

These arguments have escalated due to the economic challenges faced by the nation and the world. Will sufficient resources be available through public and private sources to enable the necessary expansion of transportation that can contribute to the increase of gross domestic production? Without sufficient transportation to move people and goods, economic growth will be stifled.

[4] Longstaff et al. (2010).

Inadequate transportation systems will also affect the delivery of goods for emergencies, disasters and catastrophes. There are inadequate highway interstate systems that were not sufficiently flexible during disasters. State Departments of Transportation are engineering transportation system modifications that will provide greater flexibility in the event of a disaster.

The state of readiness and resilience in commercial transportation logistics systems affects the level of an emergency. The greater the readiness, the greater the ability to overcome and mitigate the impact of the disaster.

Communications Systems

The importance of communication during a disaster is well known as a critical component of effective recovery. It remains one of the greatest challenges. Hurricane Katrina illustrated that a widespread disaster can strand employees without access to working landline or mobile telephone services.

The Federal Highway Administration has conducted tests on the connection between communications and disasters. Studies of evacuation behaviour find that the most typical action that people take upon receiving a message that recommends evacuation is to seek to confirm the first information they hear. Many continue to check multiple sources of information for the purpose of making sense of the situation, so they can engage in protective action. They will use whatever information they perceive to be most credible. Social media injects another phenomenon into the current communications infrastructure. Instant information is expected from smart phones and people act on first-report information.

There is a need for communications interoperability and pre-event strategic communications planning among main stakeholders. Additionally, the effective use of cloud technology in crisis management must be identified pre and post-event. Another important need is robust communications systems to communicate status of infrastructure recovery to main stakeholders.

Energy/Power

Access and reliability of power is critical in recovery. Regional networks among service providers and power stakeholders must be established, pre-event. Additionally, efforts need to be made toward improving the capability of utilities and related service providers. Finally, previous disasters and events have demonstrated the need for access to and availability of real-time grid status.

Adaptability, like resiliency, can be measured by the amount of time it takes to recover from a disaster. The adaptability of a community depends on its proximity to the impact and to recovery resources. The closer to the impact the less flexibility and adaptability a community has to recover and, adversely, having the right resources accessible in the community, the more adaptable and able to rebound after

a disaster it is. Adaptive capacity and resource robustness appear, up to a point, to be inversely related. One of the main points in understanding this relationship is also understanding the role of power in community recovery. How much time is acceptable for a community to be without power? How long should it take to restore critical operations that depend on power?

Supply Chain Delivery Challenges

Financial Resources

Customers and employees remaining in, or evacuating from, affected areas may need unexpectedly large amounts of cash to pay for critical goods and services. In anticipation of hurricanes or other disasters with advance warning, some financial institutions have developed plans for ordering larger shipments of cash prior to the expected onset. These institutions also reported the need to plan for enhanced security precautions.

During Hurricane Katrina, customers with automatic deposit and bill payment services experienced less difficulty in maintaining their accounts. Pre-disaster financial preparation, such as establishing direct deposit account relationships or automatic bill paying services, can mitigate disruptions to survivor finances. What is known is that disasters affect access to financial institutions and money and electronic forms of payment. Solutions need to examine how to credential individuals for security operations and how to ensure private-sector redundancy and preparedness.

Medical Supplies

The issue of medical supplies presents several important challenges, including the coordination and collaboration between the private and public sector on supply inventory and distribution. Additionally, an exorbitant amount of time, technology and human resources is still spent on credentialing individuals and ensuring that the appropriate medical professionals are where they need to be to support recovery efforts. Everyone must also work to establish and reach consensus among stakeholders on implementing dispensing protocols.

Pre-disaster planning and identification of resource needs are especially critical to the healthcare resource categories. Healthcare providers are naturally concerned about the lack of pre-incident planning that might align supply with the community's resource needs during short-, medium- and long-term recovery scenarios. Without pre-disaster resource planning, private-sector organisations capable of providing essential goods cannot design their plans to ensure that essential resources are available after an incident.

There are few instances, if any, where local government, local businesses and non-profits are brought together to designate predetermined suppliers, transporters

and distributors of essential goods and services – in other words, to plan collectively in support of post-disaster community recovery. The absence of these pre-established relationships, particularly regarding medical supplies, not only hinders the efficient delivery of medical supplies to the local population but also increases the risk that local businesses and non-profits will compete for the same resources during periods of limited supply.

Vital Supplies

The dilemma of market capacity is to have enough, or more than enough, inventory of any possible resource, especially vital supplies, needed to cope with an emergency. The amount and type of inventory necessary would increase in a disaster. Can there be enough inventories? Can there be too much? What is the right type of inventory and where is the inventory needed?

It is necessary to break down timelines for inventory. Recent research examines the staging of inventory based on pre-emergency considerations. This research focuses on the panic that ensues when the community is made aware of a potential emergency. Evidence of pre-emergency panic is seen at retail stores, such as home improvement stores for building supplies, generators, etc. Long queues form as the community panics.

To ensure vital supplies are available, agile and flexible, provision and distribution systems must be developed, as well as the effective management of spontaneous donations by communities and resource providers.

Potential Remedies

One of the primary disruptive approaches is how the parameters of a disaster are approached. One assertion explains that people should not respond with incident command, but rather theatre command. Theatre command can be defined as a comprehensive integration of all elements in the region of a disaster during the response and recovery phases. Supply chain resiliency is a critical component of theatre command. Theatre command is the approach taken by resilient communities and it needs to be applied to all events in all regions. It therefore provides a strategic umbrella under which the following recommendations are positioned.

Coordinating with Local Government

The lack of coordinated planning and information sharing between local government and the private sector is a major impediment to efficient recovery resource management. Because local government and the private sector do not collaborate to

identify resource needs prior to an incident or to establish communications plans to be activated in post-disaster recovery, businesses and non-profits are forced to make their own assumptions about the community's needs when a real disaster hits. Similarly, private-sector organisations are often unaware of whom to contact within local government for assistance with recovery-related issues.

- Establish relationships among main stakeholders and develop memoranda of understanding, pre-event.
- Facilitate coordinated planning and information sharing between local government and the private sector.
- Preposition relief items further down the supply chain, in the tactical zones (just outside the affected area but often inside the affected country or in a neighbouring country).[5]
- Identify pre-event regulations that impact commercial and humanitarian operations and develop memoranda of understanding to adjust them, if necessary.

Guaranteeing Availability of Essential Resources

Pre-disaster planning and identification of resource needs are especially critical to the food, animals and healthcare resource categories. Healthcare providers have raised serious concerns about the lack of pre-incident planning with local government to align supply with the community's resource needs during short-, medium- and long-term recovery scenarios. Without this level of pre-disaster resource planning, it is more difficult for private-sector organisations capable of providing essential goods to design their plans to ensure that essential resources are available after an incident.

- Convene private and not-for-profit sectors and local government to identify resource needs, pre-event.
- Minimise market panic in a disaster through price discounting, which encourages individuals to purchase items that may be in high demand during a crisis, pre-disaster.
- A variation of this strategy may be to develop cooperative purchases of essential materials that can be available in the pre-emergency hours of imminent emergencies. This approach may delay the queuing process, minimising material shortages at retail establishments and reducing panic levels.
- Base a supply chain on geographical considerations, or geographically based supply chain management, to narrow the scope of stakeholders, thereby making supply chains more manageable. Emergency managers can leverage relevant supply chains by understanding the interdependencies among geographical areas and regions, state and municipalities.

[5] Australian Council for International Development's Humanitarian Reference Group and the Australian Government (2007).

Ensuring Continuity of Supply and Balance of Goods

Another major challenge is that local government usually does not have a programme for bringing local businesses and non-profits together to designate predetermined suppliers, transporters and distributors of essential goods and services – in other words, to plan collectively in support of post-disaster community recovery. In addition to hindering the efficient delivery of recovery resources to the local population, the absence of coordinated disaster recovery planning among private-sector organisations creates the risk that local businesses and non-profits will compete for the same resources during periods of limited supply. Likewise obtaining corporate approval for local resource requests could affect the timely delivery of essential recovery resources. In response, resource providers would like to establish formal relationships with local emergency managers to hedge against possible lag time in corporate approvals.

- Establish formal relationships between resource providers and local emergency managers to hedge against a gap in delivery caused by the need to wait for corporate approval and/or other types of process-based regulations.
- Coordinate relationships between local businesses, non-profits and predetermined suppliers, transporters and distributors of essential goods; plan collectively for post-disaster recovery.
- Develop web-based tools and systems.

Incident Communication to the Public and Resource Providers

Local governments struggle to communicate information to the public regarding needed resources for disaster recovery. The result is often an influx of unneeded donations and spontaneous volunteers showing up at the scene, taking first responders away from more critical tasks. Without a functioning information management system for the acquisition, storage and distribution of recovery resources, communities will struggle to ensure the availability and timely delivery of critical goods and services after a disaster.

These challenges place a heavy burden on emergency responders during short-, medium- and long-term community recovery. Without a way to track resource needs and inventories, local businesses, non-profits and governments cannot ensure that the availability of essential recovery resources is at the right place at the right time.

- Develop functioning information management systems for the acquisition, storage and distribution of recovery resources.
- Apply tools that work successfully from a normal state to the emergency state. The emergency state must utilise applicable tools from the normal state.

- Maintain and keep current contact lists. Emergency management entities should develop, test and update a contact list for senior management, employees, customers, vendors and important government agencies. Maintaining copies of this information at all sites, plus one or more off-site locations, is critical for effective disaster management.
- Establish redundant communications. Emergency management entities should develop alternative ways for locating and communicating with employees and customers. Less-traditional communication methods might include two-way radios, mobile telephones with out-of-state area codes and/or text messaging capability, satellite telephones or personal data assistants. Employees would use these less-traditional communication methods to report their location and obtain current information. In addition, it is also important to establish a central point of contact outside the potential disaster area and make pre-established free-phone telephone numbers available for employees and customers.
- Ensure communication infrastructure and interdependency.
  - Example: While the financial system is recognised as a part of the critical infrastructure, financial institutions have to compete with the restoration of other critical components during recovery efforts. Some financial institutions have joined regional coalitions to facilitate critical infrastructure planning efforts. For instance, obtaining additional cash (a critical commodity in an affected area) can hinge on whether telecommunications and electrical services have restored power and processing capability to institutions or ATMs, the transportation authorities have reopened traffic routes and the petroleum industry has provided fuel so armoured couriers can enter and leave disaster zones.[6]
- Ensure critical information is communicated out from the emergency managers to private sector users including:
  - Real situation awareness of the status of the incident and milestones
  - Resource requirements and drop-off locations
  - Power outages and restoration time approximation
  - Communications outages and restoration time approximation
  - Transportation restrictions, including roads, closures and changes to hours of operations
  - Curfews and water bans

[6] Australian Council for International Development's Humanitarian Reference Group and the Australian Government (2007).

Delivering Essential Resources to Points-of-Need

Local emergency managers have had limited success with pre-disaster outreach to small non-profits and community organisations to establish points of contact and post-incident communications procedures. Most existing groups do not currently focus on emergency planning, but they could provide a solid foundation for pre-disaster resource planning to reach vulnerable populations in the region, such as disabled or elderly citizens or those living in remote areas. Volunteer management representatives already exist within local emergency operations centres (EOCs), but their emphasis is on personnel resources rather than the delivery of essential goods to point of need.

- Facilitate pre-disaster outreach between local emergency managers and small non-profits and community organisations to establish points of contact and post-incident communications procedures.
- Identify the distance between supplier and destination within the supply chain to assess recovery time.
- Leverage already existing volunteer management representatives within local EOCs to focus on delivery of essential goods to points of need.
- Develop alternate transportation methods.
  - Example: In the aftermath of Hurricane Katrina, many financial institutions had employees scattered across the region with limited access or means to reach the institutions' facilities. To address this issue, some institutions arranged alternate transportation methods, e.g. carpools, bus services and air connections. Some institutions also developed plans to shift and transport employees either from or into affected areas.[7]
- Ensure transportation mode redundancy. Utilise intermodal capabilities to move goods so that one mode can support another when one or more modes become unavailable. By creating modal redundancy, the routing problem can be addressed by minimising the unsatisfied demand that can occur because resources and first responders are overwhelmed,[8] thereby enabling improved and efficient delivery of goods.
- Manage inventory through the ability to reroute materials.
  - Example 1: Restaurants compete on their pricing, quality and variety. But they make their money on keeping inventory low and minimising spoilage. As stocks need to be replenished by a restaurant, the food purveyor makes the delivery within agreed business rules. Ownership of inventory rests with the purveyor until the restaurant requests the items.

[7] Federal Financial Institutions Examining Council 1).

[8] Shen et al. (2007).

– Example 2: Retail enterprises maintain their own centralised inventories to minimise the amount of inventory at a particular location. By watching point of sale data, they are able to track purchases and route trucks to restock items. This method increases the cost of transportation, but inventory savings more than makes up for the extra cost.

Conclusion

In real life, almost all decisions incorporate uncertainty about the future. Assessment of that uncertainty and, thus, the risk that is inherent in these decisions can be critical – especially in times of crisis.[9] Providing real-time granular information required for 'sense and respond' situational readiness can help assess risks in situations when information about future events or future effects of events is incomplete and imprecise.

Businesses can achieve the flexibility needed during a crisis by sharing important supply chain data with business partners. Information transparency is critical to providing visibility into product movement and understanding operational impact. In a weather-related emergency, a retailer is likely to face disruptions in receiving products allocated to, from or through affected areas. Accurate product tracking and visibility enhances the ability to locate products in the supply chain at any time. The ability for retailers, carriers and suppliers to access the same real-time tracking information helps ensure product is rerouted to a nearby facility or forward location. This capability is critical in a crisis.

Information and knowledge exchange between emergency management stakeholders and their counterparts in commercial logistics does not flow easily because of an absence of tools and vehicles for facilitating this exchange, exacerbated by long-evolved cultural differences between them. Expectations by emergency management professionals of the performance of commercial logistics are heightened by the perceived strength of logistics providers in the normal state. This strength is not easily transferable into the emergency state and therefore may raise unfulfilled expectations.

The 2007 Report, 'Getting Down to Business', published by Business Executives for National Security asserted the following finding, regarding the delivery of goods:

> America's existing commercial supply chains can provide a wider range of goods and services on demand than any level of government can possibly match. During national disasters, these supply chains have provided goods and services both with and without payment from an end user. Government at all levels should incorporate such capabilities into disaster response planning.[10]

[9] Valishevsky (2003).

[10] Business Executives for National Security (2007).

Responsiveness means accurately anticipating demand changes. In a natural disaster, demand can spike and shift unpredictably. Time to react is razor-thin. Establishing a single point of demand, instead of forecasting from several sources, can increase demand visibility. Time is not wasted reconciling information from different divisions. The supply chains of companies can respond quickly, scheduling necessary labour resources based on expected volume increases and planning for asset replenishment.

For the purposes of determining what information would be most valuable to recovery resource providers immediately following an emergency, 30 professionals who deal with supply chain matters either in normal or in an emergency were asked which real-time information items from a list would be most valuable to ensure supply chain continuity during a crisis – 93–100 % of those surveyed agreed that the following real-time information would be valuable:

- *Transportation*: detours, traffic conditions, bridge/road closures/access
- *Energy*: power/electrical outages, mobile fuel supplies
- *Telecommunications*: disruptions, Internet access
- *Resource management*: what is needed on the ground, drop-off/delivery locations, coordination with other providers
- *Infrastructure*: water conditions
- *Weather conditions*
- *Local EOC real-time situational awareness* and a mode of interfacing with EOCs in real-time, e-alert systems

Additionally, when asked to self-generate what additional real-time information was also important for continuity during a crisis, the following were given:

- Current threat status, criminal activities and responses
- Central information and data availability for real-time mapping and information sharing
- Important government agency points of contact

Probably the most valuable information captured was the challenges that private-sector supply chain managers confront in a disruption that emergency managers could 'fix', pre-event, thereby affecting the delivery of goods.

Because emergencies and all hazards are unpredictable, written plans (e.g. stockpiling medical supplies) do not create the flexibility and adaptability to a situation that is needed in real time. Dynamic models and planning are not directives that need to be taken off a shelf; rather, they are internalised by the operators, the managers and the actors and can be accessed immediately and effectively in a crisis. Additionally, they are exercised by both the public and private sector, together, pre-event.

In order for crisis management, community and regional planning to be effective, the static model of the plans and related documents that are produced must be re-examined and everyone should commit to producing dynamic models. Dynamic models are capable of shifting and evolving as resources and needs are available and they adapt to the changing nature of a crisis. It must be ensured that these models use supply chains as the foundation.

Supply chains are designed to adapt to the changes in supply and demand on a daily basis. Because this system, which responds to daily dynamic changes, is the primary infrastructure that carries resources to communities, it is only logical that it would be used as a model for unpredictable events.

Charlotte Franklin, CEcD, is Deputy Coordinator of Arlington County's Office of Emergency Management, where she is responsible for resiliency and resumption planning after disasters. Following 9/11, she spearheaded the design of the first workshops in the country's first workshops on business recovery and building threat mitigation and assessment. She is a Master Continuity Operations Planner (FEMA), is Advanced Development Emergency Manager (FEMA) and is certified as an Economic Development Professional (CEcD) by the International Economic Development Council.

Kiersten Todt is the President of Liberty Group Ventures LLC and has been the lead consultant in working in the National Capital Region on recovery resource planning and management through FEMA UASI grants working with the Northern Virginia Emergency Resource System and Regional Catastrophic Preparedness Grant Program. She is also the lead on projects for city, county and campus exercises and emergency planning.

References

Australian Council for International Development's Humanitarian Reference Group and the Australian Government (2007) Emergency response supply chain assessment

Business Executives for National Security (2007) Getting down to business. Available at http://www.bens.org/document.doc?1a=11. Last accessed 14 Feb 2014

Federal Financial Institutions Examining Council (2011) Hurricane Katrina: Preparing your institution for a catastrophic event. Available at http://www.fiec.gov/katrina_lessons.html

FEMA (2012) Strategic playbook: regional catastrophic preparedness and supply chain resilience. Available at http://www.catastrophepreparation.net/SCRS/html/StrategicPlaybook_v3.pdf. Accessed 15 Jan 2014

Holguín-Veras J, Jaller M, Perez N, Van Wassenhove L, Wachtendorf T (2012) on the unique features of post-disaster humanitarian logistics. J Oper Manag 30(7–8): 494–506

Longstaff PH, Armstrong NJ, Perrin K, Parker WM, Hidek MA (2010) Building resilient communities: a preliminary framework for assessment. Homeland Security Affairs. Volume VI, NO. 3 (September 2010) www.hsaj.org

Regional Catastrophic Preparedness Grant Program (RCPGP) (2012) Supply chain resilience interim report – catastrophic vulnerability and mitigation

Shen Z, Dessouky M, Ordonez F (2007) Stochastic vehicle rerouting problems for large-scale emergencies. Available at http://www-bcf.usc.edu/~maged/publications/routing4LSE.pdf. Accessed 11 Dec 2014

Valishevsky A (2003) Granular information-based risk analysis in uncertain situations. Available at http://citeseerx.ist.psu.edu/viewdoc/downloaD?DOI=10.1.1.12.131&REP=REP1&TYPE=PDF. Accessed 11 Dec 2013

Breach with Intent: A Risk Analysis of Deliberate Security Breaches in the Seafood Supply Chain

David Forbes and Paul Alexander

Abstract Global seafood supply chains are amongst the most complex of any, typically requiring short shelf life products to be transported long distance with stringent temperature and quality control. These requirements and large-scale outsourcing, wide-scale use of intermediaries, and often multiple transformation processes create opportunities for product quality failures, particularly at participant handover points, conversions, and transport mode changes. Failures include both degradation of the physical condition of seafood and damaged trust perceptions about its integrity and identity. These occur not only by accident, but sometimes willfully. Quality failures and negative market perceptions have the potential to do great damage in seafood supply chains with significant financial impact and even collapse of whole markets.

Much work has already been contributed on unintentional quality problems in seafood supply chains, so in this chapter we provide a review of the seafood supply chain with a focus on intentional security breaches. We examine the susceptibility to security degradation of the components of the supply chain and the forms it takes. We highlight existing mechanisms used to identify and counter these events, and we posit technologies and strategies that can be employed to minimise them.

Keywords Seafood • Supply chain • Security • Fraud • RFID • DNA

Introduction

Supply chains (SCs) are global, with many intermediaries participating, and large-scale outsourcing the norm. As the SC processes and activities are executed, every handover to new participants, every transition to a new stage, and each conversion and transport operation provides a separate opportunity for 'contaminating'

D. Forbes (✉)
Curtin University, Bentley, WA, Australia
e-mail: gojfg@msn.com

P. Alexander
Curtin Graduate School of Business, Curtin University, Bentley, WA, Australia
e-mail: p.alexander@curtin.edu.au

A.R. Thomas, S. Vaduva (eds.), *Global Supply Chain Security*,
DOI 10.1007/978-1-4939-2178-2_9

the products in the SC. There are many forms of contamination, and much effort has focused on those that relate to the quality of products. This has given rise to a significant body of literature on product quality failure (Lee and Whang 2005; Robinson and Malhotra 2005; Roth et al. 2008; Starbird and Correspondence 2001). Quality in the SC goes beyond just the physical condition of product and also includes trust in the product's integrity by intermediaries and end consumers, reliability of supply through all stages of the SC, and even questions of product identity, either through a loss of identity continuity or by willful counterfeiting.

So, SCs are subject to various product quality failures at many points, as we elaborate further on. From a security perspective, these can be divided into two broad categories: unintentional and willful quality failures. Individual SC operators all actively aim to reduce unintentional failures since these cause negative consequences that beg avoidance. Willful service failures provide opportunities for individuals in the SC to gain profit through deception of some sort. This profit will be at the expense of end consumers definitely and likely at the expense of the industries serviced by the supply chain. Nevertheless, they provide an incentive to actually create exploitable quality failures.

Whichever form quality failures take, they typically have both a direct impact on the consumer (the product's performance is not as expected) and also on market perception. Indeed, persistent quality failures can greatly change market acceptance of products delivered by SCs (Gardner 2003; Roth et al. 2008). Willful deceit too is enabled by the distributed nature of global SCs. Pharmaceuticals, for example, which are high-value items, have been targets for counterfeiting. Direct safety issues, market distortion, and product credibility have all been impacted, and for this reason, the industry has invested in high security SCs utilising integrated information systems and technology such as radio frequency identification (RFID) tags (King and Xiaolan 2007).

The effect of these quality failures, regardless of their source, is on the overall security of the SC and, if security compromises are endemic to the industry it serves, they can in the extreme present a threat to the industry's potential viability. Consider, for instance, the recent European 'horsemeat' scandal in which this source was substituted for beef and pork. Although it is estimated to have represented only a tiny percentage of the total output of the product and had no health impacts, it decimated the market with recovery not complete a year later (Premanandh 2013; Sloan and McCarthy 2013).

In this chapter we examine the SC of a globally important product, seafood, and examine its security in terms, particularly, of intentional security breaches. As this occurs in the context of quality failures, overall it is first necessary to understand how this SC operates. The seafood supply chain (SFSC) is complex, diverse, and global, and it requires stringent controls to ensure product quality end to end. Although its cost per item is typically less than that of pharmaceuticals, its sheer volume nevertheless provides many opportunities and incentives for accidental damage and even deliberate manipulation of the product. SFSCs, because they deal globally with a highly perishable product and consist of many intermediary products and agents, must be operated with continuous and stringent controls (Blackburn and Scudder 2009). In many cases seafood can also be misrepresented, since there can be large market price variations based on differences that are not easily seen. This occurs not

only at source but at any one of numerous points within the SFSC. By the time the product is accepted by end stages of the SC, including restaurants and end consumers, it may have changed its identity, for example, from that of a low-cost product such as Nile perch to a high-cost product such as Barramundi (ABC News 2005).

The SFSC is mature in that production, transport, storage, and procurement practices are well developed and continuously evolving to incorporate new practices and technology (Sankaran and Suchitra Mouly 2006). However, its complexity, distributed ownership, diversity of sources and markets, and sometimes long lead times create opportunities for security impacts outside those of direct production, transport, and storage (Grainger 2007). We therefore focus here on intentional security in those areas rather than within each stage of the SC.

In presenting our analysis, we first scrutinise the supply chain as it relates to those points most vulnerable to intentional security breach. We then examine relevant security concepts. Finally, we apply these to the SFSC in order to identify strategies that the industry can use to reduce such breaches and mitigate their negative impacts. We have adopted this method to serve as a template for analysing and identifying, in substantial SCs, intentional security vulnerabilities, and impacts.

The Global Size of Seafood Markets

The global seafood market was estimated at 158 million tonnes in 2012, a growth of 6.3 % since 2010 (Food & Agriculture Organisation of the United Nations 2014). Of this total, 18 % of production is of shrimp, 11 % of groundfish (Atlantic cod, pollock, haddock, and other species), about 8 % for each of salmon and tuna. Aquaculture now represents an increasing percentage of total production, with some sources such as Vietnam, China, and Indonesia favouring aquaculture at levels of 40–80 % of their total production.

In monetary terms, global seafood production represents $252 billion US, with export/import trade of US$ 129.5 billion in 2012, a growth of 30 % in just 3 years from 2009 (Food & Agriculture Organisation of the United Nations 2012a, b)

The Structure of the Global SFSC

SFSCs are truly global, with raw product, intermediaries, and finished goods travelling large distances from the middle of oceans, waterways everywhere, and across continents, and in the case of reprocessed products, sometimes more than once. They are complex, multinational commercial, and physical chains linking source, intermediary, and end-product suppliers, processors, sales, and other functions, with the aim of globally providing a very large range of seafood products. They embrace all stages from wild catch and harvesting through multiple processing stages to end products that take a variety of forms from simple conversion to chilled, otherwise unprocessed, products (fresh whole fish), through various levels of processing to provide many possible end products (United Nations Environment Programme 2009).

Adding significant rigour and complexity to SFSCs is the need to maintain highly reliable cold chains, in which product is temperature monitored and controlled at all times, and fresh chains, in which product is moved from source to end consumer with only chilling and minor conversion/repacking. This places significant discipline on all a SFSC's stages since seafood is highly (sometimes extremely) perishable; shelf life prior to processing of only hours is typical. Fresh seafood must therefore be transferred from source to market in extremely short times, and this leads to extreme distribution mechanisms in some cases. Live lobster, for instance, is specially packed, prepared, and air freighted, resulting in a lead time of only 4–5 days from catch to consumption (Commercial Fisheries News 1999). These rigorous requirements, compounded by global distribution of product sourced in local regions, dramatically raise distribution costs. This leads to a higher priced product and in turn to higher consumer expectations in terms of quality, presentation, appearance, location, and species-specific demand.

Even when seafood is not consumed fresh, it still requires very rapid processing prior to creating durable products that can be stored at room temperature (e.g. tinned goods), held for long periods frozen, or stored for intermediate periods (months) as chilled product. Each of these processes increases the maximum acceptable lead time across the entire chain but carries with it extreme requirements to ensure quality of product handling up to and including (in the case of chilled and frozen seafood) consumption (Australian Food and Grocery Council (AFGC) 2013). Thus, cold chains of high integrity must be operated over at least some and sometimes all of the SFSC, starting at the time of the catch.

Similar to many modern supply chains, SFSCs consist of increasingly specialised, more narrowly focused networks of globally distributed participants (United Nations Environment Programme 2009). Globalisation of SFSC supplier networks allows access to a wider range of skills, lower-cost bases, and of course global and highly diverse sources of seafood. At the consumer end, globalisation provides access to much larger market opportunities for suppliers and manufacturers and a better range and potentially lower prices to consumers, reflected in diminishing seasonal and location dependence of seafood. Specialisation (of supply chain members) allows expertise to be focused and concentrated and leads in many cases to economies of scale. It is not surprising therefore that such supply chains consist of a very large cohort of specialised transnational participants working together to send product(s) from source to end-consumer segment(s).

Risks and Complexity of SFSCs

With the inherent globalisation of much of the SFSC though are attached much increased complexities and the need to manage greater and more diversified risk. As global supply chains are physically longer than local ones, lead times are increased significantly for any given overall supply chain cost base. This places four demands on members of typical SFSCs.

Sales Demand Inaccuracies

Firstly, SFSCs must accurately anticipate sales demand much further into the future than for local chains and this becomes increasingly difficult. The longer into the future sales demand is projected (Tolbert 2012). Inaccuracies in projecting this demand lead to stock excesses and outages. This is never an optimal financial situation for supply chain members and is compensated for by carrying safety stock and placing orders for end products and intermediaries from that stock. However, long lead times increase the financial penalties associated with safety stock. In SFSCs, keeping safety stock of chilled seafood is highly problematic because of its limited shelf life, and since chilled product represents at least part of most SFSCs, it therefore precludes large-scale use of this measure except where a high level of wastage can be tolerated and paid for by the consumer. This favours reliable delivery in highly variable markets mainly for premium (i.e. expensive) seafood products, where the market is prepared to pay a premium that covers these inefficiencies. For such products it also generates strong incentive to subtly manipulate stock identity to meet supply demands.

Border Complications

In addition to increased distance travelled and the lead time associated, every border crossing seafood products and intermediaries undertake adds time, complexity, cost, and risk. Borders are commonly associated with transport/storage mode changes, for instance, transfer from a ship in port to road freight, and with inspections, checks, administrative delays, and fees. This also applies to Customs and Border Control activities, where delays can be significant and, with perishable product, can lead to spoilage and large-scale SFSC disruption. Additionally, legal requirements change at borders and affect contracts between members of the supply chain, as well as creating extra and various obligations to state entities. These regulations and conditions must be complied with across the entire SFSC, from absolute source to ultimate destination, as failure can lead at best to longer lead times and disruption and at worst to legal action and loss of product. And of course these events are all associated with extra direct and indirect costs.

Borders and the documentation required to cross them also provides opportunities for illicit intervention. Not all states operate corruption-free border control bureaucracies and these are frequent targets for attacks on intentional security.

Time-Related Unspecified Risk

Within any supply chain, each stage that product passes through carries a probability of disruption or loss of suitable product which increases as a function of time. It is a statistical inevitability based on the length of time that the product is exposed

to the risk. In other words, the longer an intermediary is in the supply chain, all other things being equal, the higher the chance of quality failures before it is handed over to the end consumer; in the case we are examining, this includes the chance of intentional security breach.

Complexity of Stakeholder Interactions

The number of participants in SFSCs is typically large, with sometimes complex physical, procedural, informational, and legal interactions. They operate within networks that may at some points be highly integrated and at others consist of arms-length transactions. In this analysis we identify seven categories of SFSC participants, each with different contributions to and requirements from other participants (Table 1). Businesses may be specialised within one of these categories or may vertically integrate several categories.

Table 1 Categories of SFSC participants

Category	Description
Logistics operators	These provide transport and storage services and facilities. There are both local logisticians who operate within the vicinity of the SFSC intermediaries and transnational ones which are able to transport and store product at a global (or large regional) level. These companies may themselves be members of coordinated networks
Raw material suppliers	This group consists of all companies that contribute components of the finished goods, including packaging and added components and the source seafood products themselves. At its broadest definition these can also include all businesses providing infrastructure (e.g. power or fuel suppliers), which, although they serve as a risk to overall supply chain operations, are generally subsumed into the SFSC as unspecified risks and typically managed by the infrastructure providers through their own supply networks
Maintenance providers	These provide services and materials that maintain the assets used to keep products moving through the supply chain
Information services providers	Provide and share information required to transfer and coordinate intermediaries through the stages of the supply chain
Supply chain managers	Provide services to optimise, coordinate, and manage the supply chain and to manage inter-company relationships
Sales agents	Find and arrange buyers and sellers of raw materials, supply chain intermediates, and final products. These have different names depending on their role and include retailers and wholesalers
Aggregators	These find and arrange ways of aggregating products and services needed in the supply chain. They are often associated with sales agents and also may have physical aggregation resources

Stages and Handover Points in the SFSC

From source to end consumer, supply chains do their work using many discrete stages, each undertaking a set of tasks that may acquire raw materials and intermediaries, convert them, manufacture them, transport them, store them, distribute them, and sell them at wholesale or retail level. Moving product from one stage to another requires controlled procedures and tasks that occur at specified handover points. Stages are typically under a single organisation's control which simplifies quality and integrity management, while handover points often require contracts and collaboration between different companies. Consequently security issues may be quite different for each of these.

Stages

Figure 1 shows the stages in the SFSC adapted from the UNEP. (United Nations Environment Programme 2009). It has evolved to be capable of supplying a large range of seafood products to diverse end-customer segments across great distances,

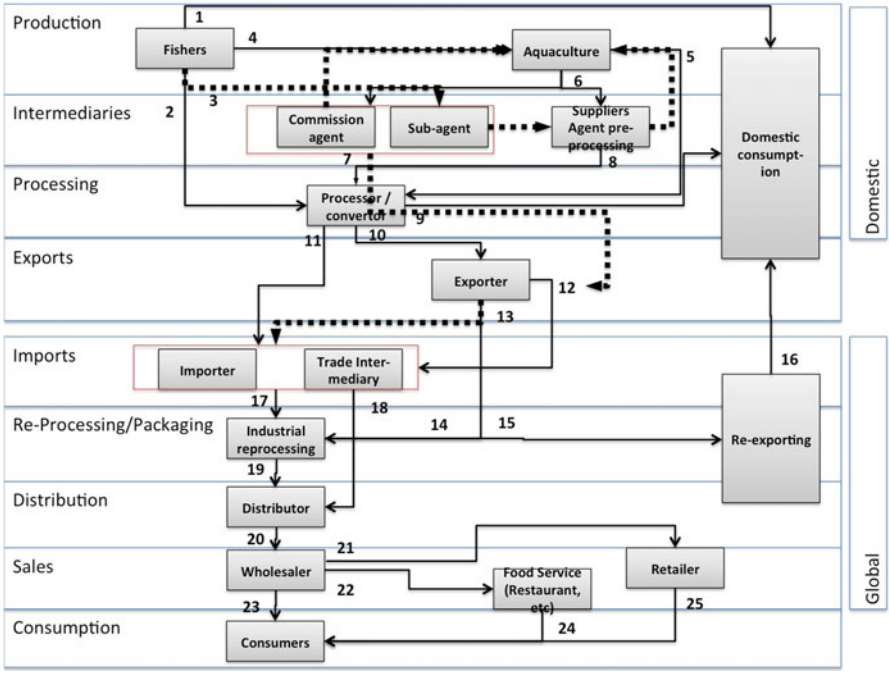


Fig. 1 SFSC showing stages and handover points (after: United Nations Environment Programme 2009, 42)

many national borders, and different cultural expectations. It has become efficient in simultaneously servicing the needs of local and global markets. The figure shows two flows, of physical product (solid lines) and information/contracts (dotted lines). As for most supply chains, the SFSC is divided into phases of production, intermediate distribution and processing, final distribution, sales, and end-consumption. In addition to these standard phases, import/export phases allow the chain to be highly responsive in a global context. Within these phases, we have identified 17 stages. Before a product leaves any stage, it must be subject to at least one handover point, and these are shown with unique numbers. We have identified 25 handover points in the SFSC.

In the SFSC physically diverse and long stages have generated the need for intermediaries who act as agents to provide aggregation, sourcing (conversion, transport, packing, and marketing) services. The supply chain as a whole, and the participants in it, must be nimble and responsive because of the short lead times in the fresh-product stages of the SFSC, which must be adaptive to changing demands and circumstances. They must also have intimate knowledge of local markets and product sources and maintain relationships that quickly and smoothly link them (Christopher 2000).

Seafood is sourced either from waterways and oceans through fishing *catches* or increasingly through aquaculture (seafood farms) by means of *harvests*. It is imperative that the harvest/catch is processed at the point it is landed (removed from the water). To achieve this requires *local processing* capabilities to convert the product to a point where integrity of the cold chain is established. At this point too, since a single source can progress through multiple and alternative supply chain stages to different end products, or the same end product but in different market segments, initial processing decisions must be made. These decisions have a direct effect on overall sales, potential profits for operators throughout the SFSC, and costs. For this reason, *preprocessing agents* are important in controlling the product flow through the supply chain. Such stakeholders work with *commission and subagents* to gate the product at this early stage.

After the raw product is stabilised (i.e. made less perishable), it can be moved and stored, which allows a proportion of it to enter the global chain. *Exporters* provide this capability. They may be directly integrated with catching/harvesting or be a separate outsourced entity. They provide expertise and resources in packaging and multimodal transport undertaken with stringent condition control. The proportion of local to exported production is generally market driven and represents a dynamic balance of local demand compared to export demand, offset by the increased costs associated with wider distribution. To mitigate those higher costs, it is common to convert the product into a more cost-effective form for export, for example, freezing fish instead of marketing it fresh.

Importing agents and intermediaries provide market-sensitive links between source producers and end customers and by so doing control the quantity, species, and destination of the whole SFSC. Some are global and others distributed locally, but all act in an integrated market. This has evolved from actual trading at physical market locations to electronic trading using large-scale integrated information

systems (Graham 1998; Sanders and Manfredo 2002). This results in a highly effective market, where product can be sourced and sent to almost any location. However, it also creates volatile pricing and demand fluctuations and can have social implications when local community-use product is diverted to higher remunerating export destinations.

Downstream from import intermediaries, *further processing, repackaging, and conversion* is often required to meet export standards, cultural differences, and market expectations and also to optimise the product for further transport and storage.

It is also possible that exported seafood will be further converted or processed and *re-exported*. This is becoming far more common, particularly for high-value seafood products, as it can take advantage of production economies of scale and access to leading edge processing technologies.

The final stages, of distributing the products to end consumers, are undertaken by *distributors,* which link seafood sources to *wholesalers* and then to *end consumers,* either directly or through *food service retailers* (restaurants, stalls, and cafes).

The Handover Points in the SFSC

Our analysis of the SFSC highlights 24 handover points in the chain (Table 2). Each of these points involves a transfer from the controlled processes of one stage to those of the next. Regardless of the security and integrity of the transferring and receiving stages, for the transfer itself to be secure, processes must exist to ensure this. If a breach occurs at this point, then everything downstream of the handover point is compromised, and in such circumstances the best possible outcome is that the compromised product is tracked down, removed, or remedied before it is reaches the end consumer, while the worst outcome is that it reaches the end consumer as somehow tainted product. In other words, the best situation is added expense and interrupted supply, and the worst is public health and market destruction. Clearly the stakes are high and the incentives strong for providing secure handover points.

Control in the SFSC

As described, inherent in the complex SFSC is the need for transfers of product to other operators and to other stages. At each of these handover points, the product is subject to one or more changes, for instance, a new process, repacking, transfer to transport medium, and so on. Handover points can also be associated with change of ownership, synchronised with physical changes, or as a discrete event. Between the handover points, the product is part of an integrated handling sequence within a stage and has a single owner (though outsourcing and contracted operations may be used by that owner). It may be production, storage, or transport related.

Table 2 Handover points in the SFSC

Handover point	Notes
1	From catch to dockside markets. Usually small scale
2	Transfer from catch to processor or convertor
3	Contractual transfer to intermediaries
4	Transfer of product as aquaculture input
5	Transfer harvest to processor or convertor
6	Transfer of harvest to supplier's agent
7	Contractual transfer to exporter
8	Transfer from agent to processor
9	Transfer for domestic consumption of processed seafood
10	Transfer to exporter
11	Transfer from processor to importer
12	Transfer from exporter to importer
13	Contractual transfer from exporter to import intermediary
14	Transfer from exporter to further processor
15	Transfer from exporter to re-exporter
16	Transfer from exporter direct to market
17	Transfer for further procession
18	Transfer to distributor
19	Transfer to wholesaler
20	Transfer to retailer
21	Transfer to food services provider
22	Transfer from wholesaler to consumer
23	Restaurant (etc.) consumption
24	Retail seafood consumption (for home cooking)

Thus, controlling the integrity of the SFSC is focused on three types of activities: those that manage the integrity of processes within the handling sequence of a single stage, those that control the obligations of ownership, and those which ensure security and quality of handover points.

Intra-stage Integrity

Sequences and processes inside a stage typically occur in an environment where operational control is high. On a (well run) fishing boat, for instance, processes, systems, monitoring facilities, and management actions are all designed to ensure the catch is landed with minimal damage, sorted, graded, stored at suitable and constant temperature, and returned to port in a timely manner. At this handover

point, responsibility and care of the product is also handed over without further consideration by the fishers. This sort of arrangement is repeated over and over from end to end through the SFSC.

In intra-stage processes, integrity is assured through internal process controls and controls administered by external bodies working on behalf of SFSC stakeholders, including industry, consumer, and government interests (Williams et al. 2003). These controls focus ultimately on three interventions to assure product identity, product quality, and product ownership.

Firstly, internal controls are based on process and engineering quality management disciplines, supported by information systems and operational management responses. They are designed to reduce defects to an acceptable level and/or to ensure traceability of the product. For instance, in manufacturing operations, statistically valid ongoing checks are performed on the production line to monitor the quality of the operation and point to changes or maintenance that must be performed (del Castillo 2002). In transport operations, tight control and documentation of stock movements helps ensure product will not be misplaced or misidentified.

Secondly, external control of intra-stage processes consists of physical inspections and documentation inspections. Its aim is to set standards that meet stakeholder requirements and to monitor their adherence (Lazer 2001). With standards, there is quite commonly a chain of transfer of these standards. For instance, legislatively defined health food regulations are translated into SFSC-specific requirements and administered/monitored by specialised industry bodies. These bodies are usually widely supported by all members of the SFSC since they provide industry input into standards and also create product trust for end consumers and therefore are critical to market acceptance of the product (Anders and Caswell 2009).

Finally, within each stage, intentional security breaches in this environment can be effected at any process, but vulnerability is higher at three specific places. Firstly, they may occur at or near the start of processes used in the stage, for example, substituting and misidentifying raw catch before processing occurs. It can also occur at the tail end of processing in the stage, where an identity switch is similarly performed for processed and potentially less obviously identifiable product. Quantities can also be manipulated here too. The third possibility is interference with compliance to standards, or even the standards themselves. This allows lower-cost/quality product to gain value by virtue of its perceived compliances.

Handover Point Integrity

Handover points consist mainly of actions required to transfer intermediary product from one stage to the next. They take comparatively little time to complete, or may even occur instantly. For instance, a handover point may consist of unloading and storing a product, transfer to a different processing operation, change of ownership, or a creation or change to a contractual obligation. We identify seven types of integrity at handover points:

Transfer Process Quality

The processes of transfer are those with properties similar to intra-stage processes. There are however typically far fewer of them, and critically, they often involve different parties. Management of quality of such processes therefore must be achieved through multiparty collaboration rather than (the much more straightforward) chain of command. Control and monitoring is generally assigned to carefully designed contractual relationships. Deficiencies in contracts can and do lead to quality compromises (Guillotreau 2004; Trondsen 1997). Intentional security breaches can exploit multiparty transactions, in particular generating some form of disinformation.

Intermediary Identity

Product identity is a significant issue at handover points, since the product must pass from one party to the next and this may rely on statements in documents or packaging without necessarily seeing the physical product. Spot checks, the potential for criminal sanctions (misrepresenting identity is after all fraud), physical management of stock, effective document controls, and audit trails to known sources are used to minimise this occurrence. Technology also plays a part and is a major use of RFIDs with the SFSC.

Quantity

Accurate quantity representation is also important. Like identity, quantity may often need to be imputed from documentation and packaging. While there is always a margin of acceptable error and loss during the handover process, there is also the potential for shrinkage (theft), package misrepresentation, and arbitrage opportunities based on different measures of quantity. As with identity, spot checks, legal sanctions, RFID technology, physical stock management, and attention to documentation also limit this likelihood.

Provenance

The source of seafood products is important as an indicator of quality and a component of the brand itself. Misrepresentation of provenance may alter perceptions of the product or lead to its mishandling further downstream in the supply chain. Quality perception even within a species may vary depending on the source. Misleading provenance may be used to rebrand intermediaries as they travel through the SFSC (Manning et al. 2006).

Provenance misrepresentation is combatted with high integrity of documentation, including legal titles. Spot checks are less useful than for some other handover point issues, intermediaries may be made to look superficially very similar. Indeed, brand differentiation can be based entirely on provenance (often location) with little or no physical distinction.

Continuous Environment Monitoring

SFSCs handle highly perishable products. Both for safety and process decision-making, it is critical that all processes are continuously monitored for exposure to conditions that may compromise its quality (and even safety). Temperature changes are the most common of these, though stacking, oxygen exposure, and other factors may be important for some products (Abad et al. 2009; Mai et al. 2012).

Many of these variations lower the product's quality and even safety, but they may not be accompanied by obvious physical changes. This provides a large opportunity for intentional security breaches.

To minimise this possibility, all seafood must be provided with a full audit trail of conditions it has been exposed to from the moment of catch and, in the case of harvesting, even prior to that process. Documentation, package-based stamps, and continuous-use certifiable environmental monitors provide such a trail. Increasingly, the use of RFID allows environmental and spatial monitoring and reporting through the use of smart tags (Abad et al. 2009).

Timing

Environmental monitoring is used to measure specific conditions required to maintain quality, but as seafood is a biological product, many complex biochemical changes occur, the vast majority of these increasing exponentially over time (Ashie et al. 1996). For each species handled by the SFSC, under particular conditions, the time for best quality is a well-established figure and is commonly referred to as the *use by* time. This figure almost always contains a margin during which product spoilage *may* not occur and is certainly not obvious except under rigorous testing. Understating the time the product has been in the supply chain therefore presents an attractive opportunity to misrepresent the product. It also places lead time limits on intermediaries and *latest time* thresholds for stages and handover points, beyond which spoilage impacts occur. As mentioned in the previous point, spoilage may not be immediately visible and therefore is a window ripe for illegal exploitation.

To combat this, date and time stamps are integrated into processing and packing processes, typically to individual item level, and this follows the product through the supply chain. To hold this information bar codes and, increasingly RFIDs, are being used, at least for outer packaging.

Title

With outsourcing and transfer to various intermediaries in the SFSC, ownership of the product changes several times. Problems with ownership may be manifested as supply disruptions downstream in the supply chain as far as end consumers. This may occur not just because of poor contracts and unclear legal title but also due to international legal mismatches. This is concerning in itself, but loss of a continuous

chain of ownership can be accompanied by loss of other controls, during which the concerns already discussed in this section can become active. Many opportunities exist to exploit these problems, ranging from allowing falsification of source locations, date of catch, species type, and so on.

Characterising 'Security' of the SFSC

Despite all the opportunities for intentional compromise of security considered above, the seafood supply industry has *in the purely physical shipment sense*, a comparatively secure operating environment compared to some supply chains. It is much less exposed to theft or diversion of product, part or whole shipments, for example, when compared with supply chains containing manufactured consumer luxury goods. The principal reason for this is that from catch/harvest to table, seafood supply is driven by time and market pressures and sensitivities. A rapid series of temperature-risk-susceptible transactions involves continuous preparation, packaging shipping, and storage actions focused on delivery of 'plate-acceptable' food product and in turn the ongoing viability of the connected SFSC stakeholder businesses. This reduces the opportunity to steal product in the traditional sense, though this of course can and has happened.

For example, processing of wild-caught seafood usually begins on board the fishing vessel. Such vessels are known as factory ships, where high-volume sophisticated operating systems complete many of the steps necessary to prepare product for market. Capabilities vary according to target fish stocks and markets served (Wikipedia. Factory ship; Wikipedia. Fish processing).

While direct theft is less likely, in such a compressed operating environment, it is reasonable to assume that there will occasionally be instances when erroneous human or machine processes result in product or species type mislabelling. Competent SFSC operators and their interdependent business relationships generally guarantee a culture of constant vigilance. It is also reasonable to believe that if discovered/reported incidents of mislabelling predominantly refer to the more expensive or more profitable species types of catch, then the likelihood of labelling error is suspect. The more perfidious of SFSC practices are not easily categorised as security issues in that purely physical containment sense.

The term 'security' in our view is synonymous with 'food safety' and 'food shipment integrity', mostly because the more significant known criminal interventions in the SFSC do not refer to stealing product but rather to adulterating it. By various means the end product is changed or substituted so that it is no longer that which it is represented when sold to a particular stakeholder. This is termed in security parlance as *economically motivated adulteration*.

Complex collaborative international partnering and geographically elongated multi-jurisdictional supply chains comprise many physical transaction locations of varying types and also complicate security monitoring capability. Examined after a

consumer impact is found, identification of the place and time of an adulteration event is elusive and very challenging for auditors or other investigators. It may also cause distributed problems and impact different species and SFSC stages.

To illustrate, in May 2012 both US and Australian test inspection reports raised alarms when various seafood products and species (shrimp, basa fillets, catfish, tilapia, and frozen fish cutlets), and imported from Asia into both countries, were found to contain enrofloxacin, chloramphenicol, and nitrofurazone, all antibiotics banned in the United States and Australia due to known and serious health implications (Avila 2012; Fyfe and Millar 2012).

Improper farming practices and the consequential effect, although undoubtedly economically motivated, do not necessarily meet the criterion for classification as fraud. But this is likely to be regarded as a breach of supply chain agreement security principles, in both a civil (stakeholder loss and risk) and criminal (jurisdictional regulatory) sense. It also has the potential to destroy confidence in multiple seafood markets, and in this case, since 90 % of shrimp is consumed in the US is imported, it can essentially kill that industry.

The antibiotics abuse detections provide a clear indication of the willingness of supply chain participants to exploit profiteering opportunities while disregarding the consequences to human health. Unfortunately government inspection capabilities and infrequency of interdiction provide little insight to the extent of deceptive practices.

Fraud: Calling the Supply Chain Problem What It Is

A number of euphemisms exist to describe what most experienced security risk managers recognise as criminal tendencies and actions that impose harm on supply chain operations, business viability, and society's consumer interests. In the global food supply chain, words such as *substitution* and *mislabelling* reflect the inability to ascribe many specific individual incidents of harm as intentional acts of fraud and theft, due to the lack of timely discovery, professional investigation, and conclusive evidence. The effective combination of those three performance metrics is greatly challenged when the supply chain represents a geographically distant, climatically diverse, and multistage handling process. Such is the case with the world's SFSC and the market it serves.

Indeed, fraud appears as an ultimate outcome of most other SFSC failures. So, although much effort (and associated literature) has focused on processes and, in recent years, particularly on RFID to maintain continuity of the product in the supply chain, and so provide integrity, we see that failures of those processes and technologies allow fraud – mislabelling and misrepresenting product – to occur. While recognising the many approaches to ensuring SFSC integrity that are available (and that we have canvassed above), we concentrate in the next section of this chapter on dealing with the ultimate fraud itself.

The Fraud Triangle

To help place our supply chain fraud discussion in context, a 1953 doctoral thesis by Donald Cressey introduced fraud deterrence and detection concepts as the 'fraud triangle.' (Cressey 1953) His three key elements in the fraud triangle are opportunity, motivation, and rationalisation. In their 1979 book on criminology, Cohen and Felson (1979) took this further and outlined a basic theory in an attempt to explain crime rates in society. They stated:

Fraud, like other crime, can best be explained by three factors; a supply of motivated offenders, the availability of suitable targets, and the absence of capable guardians—control systems or someone 'to mind the store'.

Much more recently, Kassem and Higson built on Cressey's concepts by integrating later theories from several sources into one model 'that includes motivation, opportunity, integrity, and fraudster's capabilities' (Kassem and Higson 2012).

Fraud and Technology

The Cohen and Felson (1979) theory was published at a time when the advent of now ubiquitous video surveillance, the Internet, and sophisticated Information Communications Technology (ICT) as a toolkit for fraud prevention and detection was arguably unimagined.

In this second decade of the twenty-first century, witnessing digital footage of criminal acts is commonplace through television broadcasts, World Wide Web, social media postings, and mobile phone message sharing. Effectively the continuous audiovisual and still-photo illustrations of society's criminal dimensions bring visibility to the hitherto 'invisible'. Similarly the availability of more advanced digital technology control systems offers monitoring protections, fraud deterrence, and enhanced detection capabilities. It must however be acknowledged that criminals of all shades from organised to opportunistic have also adapted and benefit today from technological capabilities that can and do defeat protection controls.

Surfacing of Security Imperatives

Our readiness to set aside a temporary thought of 'mislabelling' as the result of human or system error is driven by an increased awareness of proven criminal interventions in the SFSC. This awareness has also prompted an awakening on the part of government administrations regulators and enforcement agencies.

Briefly referenced here are the better known of the food supply chain events that have created serious public concern, revealing weaknesses in security and resulting in diminished confidence in previously trusted products and their purveyors. These happenings have thereby adversely affected businesses, as consumers change their buying habits. The immediate effect on the end of chain seller is to impose unrecoverable losses through the collapse of sales and the cost of disposal of unsold

and therefore wasted product. It takes longer for this to be felt upstream by supply chain operators, with immeasurable damage to trade and business viability.

That word 'immeasurable' is applied here in its literal sense, for no data is available to show the true consequences to stakeholders in a widely publicised food supply chain scandal. Lessons worthy of close study however do exist. These confirm the reasons for legitimate SFSC participants to introduce and sustain management systems of control to mitigate risk of criminal interventions.

The examples that follow are not explored in detail as these are comprehensively examined by numerous credible sources of expertise as referenced per exemplar. The purpose of inclusion here is to set the scene whereby any overly generous excuse of operator or system error is itself a danger to the essential quality assurance required for food safety.

Effectively, *food safety* in the supply chain environment can be regarded as synonymous with and also a beneficiary of *food security*. A critical asset for effective risk management is critical awareness. This includes and arguably prioritises the need to constantly anticipate, monitor, and evaluate security threat and risk trends. The advent of the World Wide Web, Internet, and social media dynamics has resulted in aggressive and innovative exploitation of opportunities for criminal gain. SFSCs present globally distanced food consumer communities with a degree of originator anonymity analogous with elements of Internet communications.

Although it is acknowledged that criminal exploitation of food SCs has a long history, our interest is focused on a series of events that appear to suggest a recent surge or onset of a trend in global food supply fraud; events that suggest that abuse of technology and exploitation of global supply chains have raised the stakes.

A Rude Awakening to Food Supply Chain Realities

In September 2008, in China, tens of thousands of children were hospitalised, and six died. This was the result of infant-formula milk adulterated with a synthetic chemical compound, melamine, a nitrogen-based compound used in commercial and industrial plastics and in this case used to falsify true and safe protein content. Over the following months, the crisis became the focus of attention worldwide as experts reported the dangers of damage to animal and human cells and other parts of the body, including the central nervous system. The dairy firm Sanlu which had been one of China's most trusted brands collapsed as a result of the scandal and two executives were later sentenced to death for their part. Twenty-two other dairy firms were also involved, with varying outcomes. Retrospectively it was reported that in early 2007, hundreds of pets died in North America due to pet food contamination in which melamine adulteration was to become the suspect factor. According to the Chinese Ministry of Health, in addition to the six infant mortalities, by the end of November 2008, 294,000 infants had been affected by the contaminated infant formula, with over 50,000 infants hospitalised

Reports continue to emerge indicating that as recently as 2014, the Chinese government has yet to eliminate melamine and other adulteration practices in spite of a considerable investment in corporate governance regulation. The ability of dishonest

practitioners to gain financially from dilution processes known as 'cutting' is well established (Karahalil 2014).

Coincident in 2007/2008 the world witnessed what has been termed the 'global food crisis'. Large spikes in worldwide food prices placed or kept an estimated 105 million people in a state of poverty in low-income countries. Manipulative financial speculation created a volatile surge of increased agricultural commodity costs imposing availability and affordability strictures on access to staple foods (Eugenio et al.). Such stark supply and demand pressures can prove to be a magnet for criminal enterprises and opportunistic individuals of dishonest tendency.

In January 2013 Irish food inspectors reported finding horsemeat in frozen beefburgers made in the Irish Republic and the United Kingdom. These had been sold by a number of well-known and otherwise respected UK supermarket chains. Subsequently a number of stores and companies across Europe, including major international name retailers, recalled 'beef-ready' meals, after tests found that they contained horse DNA (BBC News 2013a, c).

In the broader food markets, supply chain food frauds in recent years have been receiving media attention, but it is difficult to say with any certainty that this represents a significant increase, as opposed to an appealing and sometimes sensationalist field of news reporting that reflects journalistic discovery of common practice. There are indicators that the presence and impact of organised crime are becoming serious dimensions in the food supply chain. There is more than a hint of this within the following reports:

2013 Pork DNA found in halal sausages at London's Westminster primary school (BBC News 2013b).

2013 South Africa's Stellenbosch University study of beef-labelled products found soya, donkey, goat, and water buffalo in up to 68 % of the 139 minced meats, burger patties, deli meats, sausages, and dried meats tested (Stellenbosch University 2013).

2014 Thousands of tonnes of fake food and drink seized in Interpol-Europol operation (Europol 2014).

From these and other food fraud reports reviewed, we have observed that the published coverage almost exclusively focuses on public harm and on the more dramatic enforcement events. Very limited information is offered on the specific methodologies used to compromise supply chain integrity. In short, the detail of criminal interventions and diversions is not widely shared, but it is reasonable to expect that enforcement and prosecuting agencies have and will acquire this knowledge.

Known or Suspected Organised Crime Connections with Seafood Fraud

Arguably more insidious that the Europol-raided organised food fraud cartels is the existence of kidnapping by organised crime gangs of young children, who are then forced into working on board fishing vessels. Adults and young people are also abducted from African, South East Asian, and Asian coastal states (Platov 2014).

Their work can be dangerous, as is the case of seine fishing when they are forced to enter the ocean to drive fish into dragnets. Reports claim that while these are not fishing boats or factory ships within the world's legitimate fisheries industry fleets, they are often crewed by experienced sailors and former fishing fleet employees. These individuals have the required knowledge and experience to help criminals circumnavigate interception by enforcement agency vessels, and the seacraft employed serve multiple criminal functions, seafood being the least profitable.

People smugglers and drug traffickers are masked by the facade of a fishing enterprise. Contamination and other hazardous practices of these criminal operations represent a threat to seafood safety and human health. Interactions and transactions occurring with legitimate seafood supply chains and processors and onward selling buyers are likely, along with adulteration risks, from illegal, unregulated, and unreported (IUU) fishing.

The Oceana Seafood Fraud Investigations

A very strong contribution to investigation of seafood fraud comes from a non-profit organisation, Oceana, founded in 2001 and based in Washington DC. Oceana is the largest international organisation focused solely on ocean conservation. This embraces protection of fish species and an ongoing battle against overfishing, including illegal, unregulated, and unreported (IUU) fishing.

Between 2010 and 2012, Oceana conducted an extensive seafood fraud investigation and in the process collected more than 1,200 seafood samples from 674 retail outlets in 21 states (Warner et al. 2013). The purpose was to determine if the samples were honestly labelled. DNA testing on behalf of Oceana found that one-third (33 %) of the 1,215 samples analysed nationwide were mislabelled in the context of standards set in US Food and Drug Administration (FDA) guidelines. Interim reports of findings were reported in the media of major cities where mislabellings were identified. In Pennsylvania 56 % of samples were mislabelled, and in Southern California it was 52 %. Of the 56 fish types tested overall, mislabelling was found in 27 (59 %). Snapper (87 %) and tuna (59 %) were the most commonly mislabelled fish types. Of serious hazard concern was the finding that 84 % of the fish samples labelled tuna were actually escolar, which is known to cause serious digestive issues.

Clearly, misrepresentation is beyond significant. In some cases it has become the norm.

Contemplating Anti-fraud Measures

For its DNA sampling and testing regime, Oceana relies upon collections by many volunteers and is establishing protocols for future regulatory and enforcement planning. With potential litigation and prosecutions as an enforcement outcome, admissibility of evidence of sample chain of custody and DNA validation demands a high standard of investigatory disciplines (Warner 2014).

Oceana is still in a growth phase and although represented in several parts of the world has yet to establish a presence in the Indo-Pacific region, including Australasia.

In the United States, two pieces of legislation are intended to combat seafood fraud. The Lacey Act makes it unlawful for a person to falsely identify any fish that has been, or is intended to be, imported, sold, purchased, or received from any foreign country or transported in interstate or foreign commerce. The Food Drug and Cosmetic Act prohibits the alteration or removal of the whole or any part of the labelling of food, if such act is done while such article is held for sale after shipment in interstate commerce.

Seafood import data for the United States is available via FishWatch, which is maintained by National Oceanic and Atmospheric Administration (NOAA) Fisheries in Washington DC. NOAA is the leading authority for US marine fisheries management. More than 86 % of seafood consumed by Americans is imported; half of which is wild-caught, and around 91 % of shrimp is imported. A summary of the prevailing seafood import situation from FishWatch reads:

> The United States mainly imports seafood from China, Thailand, Canada, Indonesia, Vietnam, and Ecuador. Our top imports (by volume) include shrimp, freshwater fish, tuna, salmon, groundfish, crab, and squid. Trade tracking programs monitor the international trade of some species such as bluefin tuna, swordfish, bigeye tuna, and Chilean sea bass by requiring that imports include documentation of details on catch—such as what gear was used, and when and where the fish was caught (NOAA 2014).

A 2013 notice from the National Fisheries Institute (NFI) website www.aboutseafood.com cited the US Food and Drug Administration (FDA) Federal Register recording of convictions spanning 2011–2013 against four men and three businesses for seafood fraud. It showed that two individuals who were owners of a company named Culinary Specialties conspired with another from United Seafood, Inc., and a fourth man representing Sea Food Center to mislabel and sell approximately 500,000 lb in weight of shrimp valued at more than $400,000. The mislabelled shrimp was ultimately sold to supermarkets in the Northeastern United States (National Fisheries Institute 2013).

Certain species of shrimp have greater retail and restaurant value than others, often determined by subtype and source location. If a cheaper type is substituted, then a larger profit is gained by the seller. The Federal Register entry referring to the above conspiracy reads:

> …instructed employees at Sea Food Center's Tampa facility to divide the shrimp received from Thailand, Malaysia, and Indonesia into smaller portions, and mark them as "Shrimp, product of Panama," on the individual packages, and then place them in boxes, also marked as "Shrimp, product of Panama." (Dept Health & Human Services 2013)

The same NFI (aboutseafood.com) web page notice referenced a November 19, 2012, FDA warning letter to Jing Sheng Company in California. It warned the company that species substitution causes their product to be adulterated and misbranded contrary to various Regulatory Acts. The FDA found that a product labelled as 'naturally cooked abalone' was actually sea snail meat. Jing Sheng Company was also cited for other labelling violations regarding the nutrition facts panel, ingredient statement, and dual-language requirements.

Regulatory Posture Transition in SFSC Security Standards

In the food safety human health–related environment, a natural and reasonable expectation is that society is protected against seafood fraud through national regulation and enforceable international agreements. Problematic for that mindset is that in common with so many facets of modern life, laws that overly depend on self-regulation by the industry are inadequately enforced. Laws and enforcement resources are overtaken by infected industry cultural downshifts in social values and tolerance of manipulation. Reduced personal integrity and increased materialistic greed bring consequences affecting supply chains. Corruption too often does not receive widespread publicity until a serious consequence to human life cannot be ignored or when major penalties are imposed on well-known business operators (Lawson 2012).

Reactive reporting of serious consequences after the fact is much less satisfactory than an effective prevention policy and practice programme. Fraud prevention approaches however are seriously challenged by the considerable complexities and operational and jurisdictional dimensions of the seafood industry. When we look for opportunities for effective improvement in consumer seafood safety, we are forced to make choices. That is:

- What are the primary human-hazard threat and harm priorities that justify more concentrated global to local seafood fraud prevention and interdiction operations?
- Which supply chain routes, participatory stakeholders, and assets (by historical threat reputation/definition), should be key targets for prevention, interdiction, and the most punitive legal measures?
- How can international regulatory and enforcement agencies overcome known jurisdictional barriers to seafood fraud prevention, interdiction, and prosecution?
- What methods, know-how, and technologies are available and known to offer cost-efficiencies in countering seafood fraud, with persuasive effect for the promulgation of inter-jurisdictional global agreements?

One option that might be enacted as a filtering strategy aimed at productive targeting is to narrow the concentrated effort down to a specific popular and thereby upper pricing bracket seafood type and its most prolific supply chain sources. One example is the substitution of King Prawn with Vannamei Prawn. The latter is a less expensive mostly mass-farmed type of shrimp. The word ‘King’ can also be confusing. It refers to a species type, not to its size.

Recognition of Hazards

The US Food and Drug Administration (FDA) published the table below illustrating in synopsis the risk associated with seafood species substitution, described as ‘misbranding’ (Table 3).

Table 3 Misbranding seafood effect

Table 3-1			
The effect of misbranding through species substitution on the identification of potential species-related hazards			
Actual market name of product	Potential species-related hazards associated with the actual product (from Table 3-2)	Product inappropriately labeled as	Potential species-related hazards that would be identified based on inappropriate species labeling (from Table 3-2)
Escolar	Gempylotoxin histamine	Sea bass	Parasites
Puffer fish	Tetrodotoxin paralytic shellfish poisoning	Monkfish	Parasites
Spanish mackerel	Parasites	Kingfish	None
	Histamine		
	Ciguatera fish poisoning		
Basa	Environmental chemical contaminants and pesticides	Grouper	Parasites ciguatera fish poisoning
Grouper	Parasites ciguatera fish poisoning	Cod	Parasites

Source: Table 3-1: US Food and Drug Administration (2011)

Three further tables in the cited FDA document extend the hazards data, viz.
Table 3-2, 'Potential vertebrate species-related hazards'
Table 3-3, 'Potential invertebrate species-related hazards'
Table 3-4, 'Potential process-related hazards'

Contemporary Regulatory and Enforcement Moves by Government(s)

Recognition of hazardous threats from corruption of the SFSC and the response processes have accelerated.

The United States of America

In May of 2014 the US FDA published details of the Operational Strategy for Implementing the FDA Food Safety Modernization Act (FSMA) (US Food and Drug Administration (FDA) 2014t). The following extracts are taken from the announcement:

Drivers of Change in FDA's Food Safety Role

> Congress enacted FSMA in response to dramatic changes over the last 25 years in the global food system and in our understanding of foodborne illness and its consequences,

> including the realization that preventable foodborne illness is both a significant public health problem and a threat to the economic well-being of the food system.
>
> The central external force driving change is the dramatic expansion in the global scale and complexity of the food system. Hundreds of thousands of growers and processors worldwide are producing food for the U.S. market, using increasingly diverse and complicated processes, managing complex and extended supply chains, and making millions of decisions every day that affect food safety. The burgeoning scale and complexity of the food system make it impossible for FDA on its own, employing our historic approaches, to provide the elevated assurances of food safety envisioned by FSMA and needed to maintain a high level of consumer confidence in the safety of the food supply. (US Food and Drug Administration (FDA) 2014t)

United Kingdom and Europe

In the United Kingdom and the wider European Union, as a consequence of the horsemeat scandal, increased attention is being given to food safety and food supply chains. In the United Kingdom Professor Chris Elliott was appointed by the UK government in June 2013 to review the integrity and assurance of food supply networks. His December 2013 interim report includes as Table 1 a copy of Young's Seafood Limited 'Seven Sins of Fish', listing the following headings:

- Species substitution
- Fishery substitution
- Illegal, unrecorded, unregulated (IUU) substitution
- Species adulteration
- Chain of custody abuse
- Catch method fraud
- Undeclared product extension (Elliott 2013)

The scheduled June 2014 Elliott Review final report has not been available for evaluation at this writing.

In December 2013 the European Parliament produced a report on 'the food crisis, fraud in the food chain, and the control thereof' (European Parliament Committee on the Environment 2013). The report contains a motion for a European Parliament Resolution for a bill to enact stronger laws to counter food supply chain fraud. It includes reference to the mislabelling of seafood products. The long listing of legislative terms mostly prefaced 'whereas' discloses the acknowledgement of prior neglect of attention to food fraud, and demonstrates that regulation and enforcement has been lacking, warnings ignored; and it includes the words 'deplores the fact that combating food fraud is a relatively new issue on the European agenda'.

During 2013 Professor Elliott contributed to a discussion on food fraud and the key role of food scientists and technologists in supporting fraud prevention hosted by Food Science and Technology online reference Griffiths (2013). One of the other contributors was John Spink, who has developed a table of types of

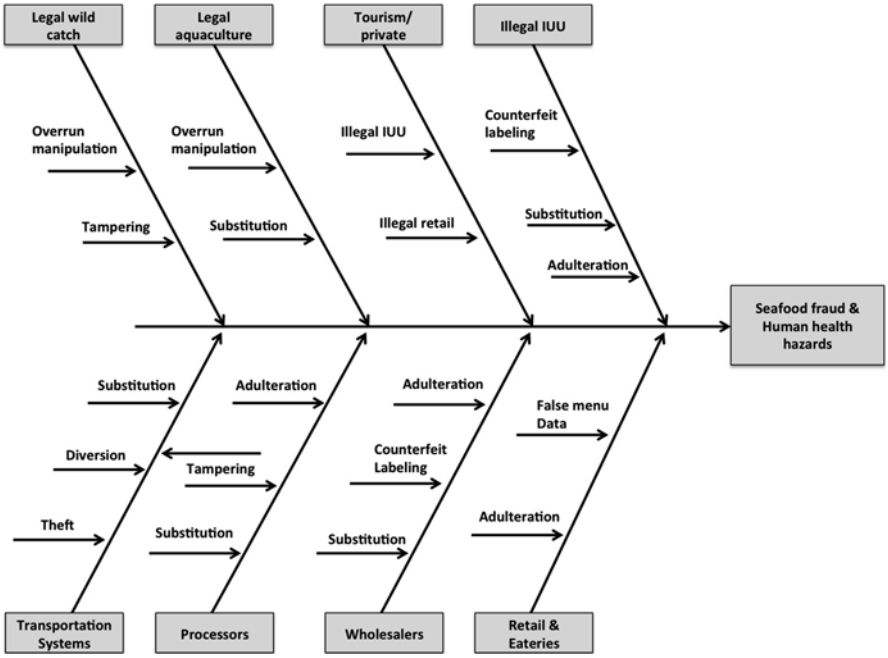


Fig. 2 Seafood supply chain fraud cause and effect 'fishbone' diagram

counterfeiting (Spink et al. 2013, 2014) which we have subsequently used as a source for the Ishikawa-based fishbone diagram of cause and effect for seafood fraud at Fig. 2 below:

DNA as a Major Seafood Fraud Combat Weapon

DNA analysis has revolutionised the identification of biological source materials. Every species and subspecies has a unique DNA fingerprint which may also identify co-related species and provide information on states of biological decay. For example, a DNA analysis can determine the exact species of a fish to a localised variation, assist in determining the nature and quantity of bacteria, and even determine if the fish is undergoing biological breakdown. DNA analysis has proved to be a powerful tool for forensic scientists charged with source identification and matching of samples, including seafood. The US FDA provides a web-based resource known as the Regulatory Fish Encyclopedia (RFE) to aid in the identification of commercially important species of fish. Building on this is FDA investment in the development of a DNA barcode database. DNA bar coding is a process by which sampling and analysis enable discrimination between different species, achieved through the use of short, standardised gene fragments (US Food and Drug Administration 2011).

The World Wide Web offers a very high volume of data on DNA analysis, and the related forensic science is rapidly developing with new knowledge being shared globally. The necessary and essential protocols and processes for DNA investigative work impose fairly high costs with skilled professional laboratory engagement and a chain of secure continuity of samples to ensure validation of findings and preservation of admissible evidence in the event of litigation or prosecution objectives.

Initiating an investigation of suspected seafood fraud samples presents a number of challenges, beginning with justification for intervention by authorised or perhaps ad hoc motivations of civil and/or criminal investigators. Protracted processes can become disincentives to the bold interventions that are called upon to penetrate criminal enterprise operations. We have in particular set out to discover whether a speedier process of DNA identification may be available, if not to categorically confirm or eliminate an instance of fraud, instead to strengthen justification for actively pursuing an investigation.

Key to the integration of DNA testing into security of food supply chains is the reduced cost and increased portability of DNA testing. A notable example is the EzyAmp device developed by SpeeDX (Linardy 2014). The device will ultimately allow doctors, researchers, and, for example, border security to identify samples within 10 min. EzyAmp (short for enzymatic amplification) can be used to quickly identify pathogens, bacteria, animals, and plant life on-site without the need to send DNA samples to a lab.

This kind of technology provides for greater efficiencies in seafood fraud detection work through integration of methodologies that could simultaneously identify the presence, if not the precise profile, of hazardous pathogens, metals, and allergens in addition to DNA species identification or elimination.

A realistic goal these devices will achieve is the introduction of time and cost-efficient seafood fraud countermeasures from detection to a more effective deterrent and prevention modus operandi on the part of regulatory, business, and consumer stakeholders' global communities.

Elevating Agency Strategies to Counter Seafood Fraud

The enormity of the security challenge for legitimate stakeholders will be apparent from the foregoing discussions. Calls for implementation of traceability measures are growing, from within and without the seafood industry (Jain 2014). DNA analysis, while undoubtedly a powerful tool in the detection process, requires reinforcement of its potential through development systems and international agreements that enable regulators and enforcement agencies to home in on the specific places and offenders in the SFSC. Ultimately the real power is in exacting punitive measures where serious instances of seafood fraud and dangerous human health hazards are proven. But governments generally do not have a good reputation for vigilance and for inspection rates or levels of prosecution that match the evidence of widespread fraud.

One day in the future, a consumer group choosing to contract with an environmental diagnostics analysis laboratory may provoke unforeseen market force penalties. Samples taken at the retail outlet or restaurant, professionally and scientifically protected after a handheld device has instantly suggested adulteration, substitution, or other criminal misrepresentation, may lead to sanctions against supermarket chains. The power resides at the point of consumption, downstream. The pain of publicity, loss of sales, and cost of seafood waste disposal will be felt upstream. Each stakeholder in the chain must police the quality assurance of the closest upstream link as well as its own operational security.

Viewing the Antifraud Horizon

The following suggested actions ensue from this research. These reflect our concern that to a great extent, agencies on which we depend for food safety have not been effective in policing the supply chains, and accordingly for criminal groups, seafood fraud has become and is currently a growth industry.

Supply Chain Security Goals for Stakeholders

- Establish and promote system to validate seafood species identity and source per transaction.
- Respect and strictly observe consumer food protection laws of source and destination markets.
- Prevent biological, chemical, or other human health hazard agent contamination of seafood products.
- Minimise disruptions of supply chains.
- Prevent co-mingling of contraband with seafood shipments.
- Prevent unauthorised access to seafood products and supply chain network.
- Prevent illegal use of transportation assets.
- Block transactions, applying zero tolerance with suspected illegal, unregulated, and unreported fishing sources.

Supply Chain Security Goals for Regulators and Enforcement Agencies

- Upgrade legal compliance requirements and licensing.
- Aggressively pursue international agreements on enforcement and penalties, including asset seizures of illegal fishing operations.
- Incentivise industry standards compliance benefits product traceability through ‘known shipper’ and ‘known shipment’ principles similar to air cargo security.

- Modernise data collection and data analysis management systems, using big data analytics.
- Build a real-time global commercial fishing activities risk and response evaluation system.
- Utilise global satellite monitoring systems.
- Introduce and maintain 'remote inspection' product tagging and tracking, applying cloud-based correlative data systems.
- Provide regulatory and enforcement agencies with leading edge, scientifically accredited detection, and analytical evidence evaluation toolkits.
- Conduct multilateral intensive targeted well-resourced, detection, inspection, and prosecution operations overcoming global logistics challenges in the process
- Impose heavy penalties on weakest links in the supply chain, i.e. where fraud is found but origin is not identified, force commercial stakeholders to seriously contemplate discontinuation of existing chain relationships

Concluding Remarks

With just a glimpse into the world of seafood fraud, this chapter has outlined a picture of supply chains that have long outrun effective regulation and enforcement and which require modernising in the risk management context. There has been an air of suddenness, even shock, surrounding the reported impact of the 2008 global food crisis; of the infant-formula melamine adulteration scandal of the same year; and of the 2013 European horsemeat scandal. The lagging, ad hoc efforts of governments to recognise and prioritise measures to fight seafood fraud and to confront risks and threats to food safety are giving way to greater focus on global supply chain security. Spanning those years since 2008, evidence of harm and future potential for harm has become inescapable, thanks to the World Wide Web and the resultant sharing of information about seafood fraud with consumers, augmented by the investigative work of scientists committed to preservation of the world's oceanic life and fish stocks.

The fuse of this new government engagement has been primed through greater consumer awareness and industry calls for stronger enforcement. On June 17, 2014, President Obama announced a new initiative to fight seafood fraud and the creation of a task force reporting to Secretary of State John Kerry to 'Prevent, Deter and Eliminate Illegal, Unreported and Unregulated (IUU) Fishing; strengthening coordination and implementation of existing authorities to combat IUU fishing and seafood fraud' (The White House Office of the Press Secretary 2014)

From a virtually invisible activity, the SFSC is now much more exposed to consumer scrutiny, as is the ability or otherwise of the agencies charged with protection of food safety measures. The case for innovative cost-efficient universally accepted ICT-driven accountability measures is gaining strength, and the greater presence and traction of DNA analysis capabilities along with integrated pathogen, metals, and allergen detection systems will deliver the desired outcomes, albeit at a cost that must be absorbed by the markets. Critical mass deployment of such applications

will in time provide a return on investment. Coupled with the genuine commitment of ethical entrepreneurial aqua farmers, government incentives for good risk management can boost confidence in the world's seafood production capacity, with a less harmful impact on ocean wild stocks.

References

Abad E, Palacio F, Nuin M, González de Zárate A, Juarros A, Gómez JM, Marco S (2009) RFID smart tag for traceability and cold chain monitoring of foods: demonstration in an intercontinental fresh fish logistic chain. J Food Eng 93(4):394–399. doi:http://dx.doi.org/10.1016/j.jfoodeng.2009.02.004

ABC News (2005) Butcher fines for selling Perch as Barramundi. Retrieved April 2014, from http://www.abc.net.au/news/2005-07-12/butcher-fined-for-selling-perch-as-barramundi/2057004

Anders SM, Caswell JA (2009) Standards as barriers versus standards as catalysts: assessing the impact of HACCP implementation on U.S. Seafood imports. Am J Agric Econ 91(2):310–321. doi:10.1111/j.1467-8276.2008.01239.x

Ashie INA, Smith JP, Simpson BK, Haard NF (1996) Spoilage and shelf-life extension of fresh fish and shellfish. Crit Rev Food Sci Nutr 36(1–2):87–121. doi:10.1080/10408399609527720

Australian Food and Grocery Council (2013) The Australian food Cold Chain logistic Guidelines 2013 (draft). Retrieved April 2014, from https://www.scribd.com/doc/239069716/Draft-Food-Cold-Chain-Logistics-Guide-Afgc-2013

Avila J (2012) Antibiotics illegal in the US found in samples of foreign shrimp. Retrieved April 2014, from http://abcnews.go.com/Health/antibiotics-illegal-us-found-samples-foreign-shrimp/story?id=16344514#.T7vcBVHwcqZ

BBC News (2013a) Horsemeat scandal: withdrawn products and test results. Retrieved April 2014, from http://www.bbc.com/news/world-21412590

BBC News (2013b) Pork DNA in halal sausages at Westminster primary school. Retrieved April 2014, from http://www.bbc.com/news/uk-england-london-21791513

BBC News (2013c) Q&A: Horsemeat scandal. Retrieved April 2014, from http://www.bbc.com/news/uk-21335872

Blackburn J, Scudder G (2009) Supply chain strategies for perishable products: the case of fresh produce. Prod Oper Manag 18(2):129–137. doi:10.1111/j.1937-5956.2009.01016.x

Christopher M (2000) The agile supply chain: competing in volatile markets. Ind Mark Manag 29(1):37–44. doi:http://dx.doi.org/10.1016/S0019-8501(99)00110-8

Cohen L, Felson M (1979) Social change and crime rate trends: a routine activity approach. Am Sociol Rev 44(4):588–608

Commercial Fisheries News (1999) Shipping live lobsters. Retrieved April 2014, from http://www.lobsters.org/ldoc/ldocpage.php?did=420

Cressey DR (1953) Other people's money. Patterson Smith, Montclair

del Castillo E (2002) Statistical process adjustment for quality control, Wiley series in probability and statistics. Wiley, New York

Dept Health & Human Services (2013) Federal Register Notices: Adrian Vela: Debarment Order. Department of Health and Human Services Food and Drug Administration, Washington, DC

Elliott C (2013) Review into the integrity and assurance of food supply networks – interim report. HM Government (UK), London

European Parliament Committee on the Environment, P. H. a. F. S (2013) On the food crisis, fraud in the food chain and the control thereof (European Parliament, Brussels ed.): European Parliament Committee on the Environment, Public Health and Food Safety

Europol (2014) Thousands of tonnes of fake food and drink seized in Interpol-Europol operation. Retrieved April 2014, from https://www.europol.europa.eu/content/thousands-tonnes-fake-food-and-drink-seized-interpol-europol-operation

Food & Agriculture Organisation of the United Nations (2014) The state of world fisheries and aquaculture (2014). In: FAO (ed) Rome

Fyfe M, Millar R (2012) Alarm at antibiotics in fish imports. Retrieved April 2014, from http://www.theage.com.au/national/alarm-at-antibiotics-in-fish-imports-20120529-1zhfw.html

Gardner B (2003) U.S. Food quality standards: fix for market failure or costly anachronism? Am J Agric Econ 85(3):725–730. doi:10.1111/1467-8276.00475

Graham I (1998) The emergence of linked fish markets in Europe. Electron Mark 8(2):29–32. doi:10.1080/10196789800000023

Grainger A (2007) Supply chain security: adding to a complex operational and institutional environment. World Cust J 1(2):17–29

Griffiths S (2013) Defining food fraud prevention to align food science and technology resources. Food Sci Technol (Online). Retrieved April 2014, from https://fstjournal.org/features/27-4/food-fraud

Guillotreau P (2004) How does the European seafood industry stand after the revolution of salmon farming: an economic analysis of fish prices. Mar Policy 28(3):227–233. doi:http://dx.doi.org/10.1016/j.marpol.2003.07.001

Jain M (2014) Investing in seafood traceability: why aren't investors and seafood businesses doing more? Retrieved April 2014, from http://newswatch.nationalgeographic.com/2014/05/12/investing-in-seafood-traceability/

Karahalil B (2014) Melamine toxicity and safety issues related to infant formula. J Trans Toxicol 1(1):72–75

Kassem R, Higson A (2012) The new fraud triangle model. J Emerg Trends Econ Manag Sci (JETEMS) 3(3):191–195

King B, Xiaolan Z (2007) Securing the pharmaceutical supply chain using RFID. Paper presented at the Multimedia and Ubiquitous Engineering, 2007. MUE '07. International Conference on Multimedia and Ubiquitous Engineering, Seoul, 26–28 April 2007

Lawson L (2012) Corruption and bribery threaten global supply chains. Retrieved April 2014, from http://www.b2b.com/2012/05/17/corruption-bribery-supply-chains/

Lazer D (2001) Regulatory interdependence and international governance. J Eur Public Policy 8(3):474–492. doi:10.1080/13501760110056077

Lee HL, Whang S (2005) Higher supply chain security with lower cost: lessons from total quality management. Int J Prod Econ 96(3):289–300. doi:http://dx.doi.org/10.1016/j.ijpe.2003.06.003

Linardy E (2014) Interview of SpeeDX. In: Forbes D (ed)

Mai NTT, Margeirsson BÖR, Margeirsson S, Bogason SGÉT, SigurgÍSladÓTtir SÖF, Arason SÓN (2012) Temperature mapping of fresh fish supply chains – air and sea transport. J Food Process Eng 35(4):622–656. doi:10.1111/j.1745-4530.2010.00611.x

Manning L, Baines R, Chad S (2006) Quality assurance models in the food supply chain. Br Food J 108(2):91–104

National Fisheries Institute (2013) FDA debars importer guilty of fraudulent mislabeling the country of origin of shrimp. Retrieved April 2014, from http://www.aboutseafood.com/content/fda-debars-importer-guilty-fraudulent-mislabeling-country-origin-shrimp

Food & Agriculture Organisation of the United Nations (2012a) Fishery production: estimated value by groups of species. Retrieved April 2014, from ftp://ftp.fao.org/FI/STAT/summary/default.htm

Food & Agriculture Organisation of the United Nations (2012b) Total value of international trade of seven fishery commodity groups, by continent, by countries or areas. Retrieved April 2014, from ftp://ftp.fao.org/FI/STAT/summary/default.htm

National Oceanic and Atmospheric Administration Fisheries (2014) U.S. Seafood Facts. Retrieved April 2014, from http://www.fishwatch.gov/wild_seafood/outside_the_us.htm

Platov V (2014) Transnational organized crime in the fishing industry. New Eastern Outlook

Premanandh J (2013) Horse meat scandal – a wake-up call for regulatory authorities. Food Control 34(2):568–569. doi:http://dx.doi.org/10.1016/j.foodcont.2013.05.033

Robinson CJ, Malhotra MK (2005) Defining the concept of supply chain quality management and its relevance to academic and industrial practice. Int J Prod Econ 96(3):315–337. doi:http://dx.doi.org/10.1016/j.ijpe.2004.06.055

Roth AV, Tsay AA, Pullman ME, Gray JV (2008) Unraveling the food supply chain: strategic insights from China and the 2007 Recalls*. J Supply Chain Manage 44(1):22–39. doi:10.1111/j.1745-493X.2008.00043.x

Sanders DR, Manfredo MR (2002) The white shrimp futures market: lessons in contract design and marketing. Agribusiness 18(4):505–522. doi:10.1002/agr.10035

Sankaran JK, Suchitra Mouly V (2006) Value-chain innovation in aquaculture: insights from a New Zealand case study. R&D Manage 36(4):387–401. doi:10.1111/j.1467-9310.2006.00441.x

Sloan E, McCarthy D (2013) FSAI: the aftermath of the horse meat incident. In: FSAI (ed) Food Safety Authority of Ireland (FSAI), Dublin

Spink J, Moyer DC, Park H, Heinonen JA (2013) Defining the types of counterfeiters, counterfeiting, and offender organizations. Crime Sci 2:8

Spink J, Moyer DC, Park H, Heinonen JA (2014) Development of a product-counterfeiting incident clustering tool. Crime Sci J 3(3):1–8

Starbird SA, Correspondence (2001) Penalties, rewards, and inspection: provisions for quality in supply chain contracts. J Oper Res Soc 52(1):109–115

Stellenbosch University (2013) SA consumers also cheated with meat products, SU study finds. News Blog Stellenbosch University. Retrieved April 2014, from http://blogs.sun.ac.za/news/2013/02/25/sa-consumers-also-cheated-with-meat-products-su-study-finds/

The White House Office of the Press Secretary (2014) Presidential memorandum – comprehensive framework to combat illegal, unreported, and unregulated fishing and seafood fraud. The White House Office of the Press Secretary, Washington, DC

Tolbert F (2012) The seven deadly sins of sales forecasting. APICS News, 28 Mar 2012

Trondsen T (1997) Value-added fresh seafood: barriers to growth. J Int Food Agribus Mark 8(4):55–78. doi:10.1300/J047v08n04_03

US Food and Drug Administration (2011) Food – DNA-based Seafood Identification. Retrieved February 2014, from http://www.fda.gov/food/foodscienceresearch/dnaseafoodidentification/ucm238880.htm

U.S. Food and Drug Administration (2011) Chapter 3. Potential species-related and process-related hazards. In: Fish and fisheries products hazards and controls guidance, 4th edn. U.S. Food and Drug Administration, Silver Spring

United Nations Environment Programme (2009) The role of supply chains in addressing the global seafood crisis. UNEP DTIE, Sustainable Consumption and Production Branch, Paris

US Food and Drug Administration (FDA) (2014t) Operational strategy for implementing the FDA food safety modernization act (FSMA) protecting public health by strategic implementation of prevention-oriented food safety standards. US Food and Drug Administration (FDA), Washington, DC

Warner K (2014) The impact of DNA Testing. In: Forbes D (ed) Unpublished

Warner K, Timme W, Lowell B, Hirshfield M (2013) Oceana study reveals seafood fraud nationwide. Oceana, Washington, DC

Wikipedia. Factory ship. Retrieved April 2014, from http://en.wikipedia.org/wiki/Factory_ship

Wikipedia. Fish processing. Retrieved April 2014, from http://en.wikipedia.org/wiki/Fish_processing

Williams AP, Smith RA, Gaze R, Mortimore SE, Motarjemi Y, Wallace CA (2003) An international future for standards of HACCP training. Food Control 14(2):111–121. doi:http://dx.doi.org/10.1016/S0956-7135(02)00115-9

The Role of Suez Canal Development in Logistics Chain

Hussein H. Abbas and Abd El Halim Omar Abd El Halim

Abstract This chapter provides an overview of existing and planned maritime infrastructure in the Red Sea. It describes the evolution of the international market in terms of supply and demand and the prevalence in maritime transport compared to other methods of transport. It then debates whether the infrastructures in the Red Sea are able to absorb the expected increase in trade flows or should we expect in the medium term that the Asian economy growth and the international trade bend.

The main focus of the chapter deals with the discussion of the risks and opportunities which exist in the Suez Canal Regional Development megaproject. It covers the issues broadly from logistics activities to maritime transportation systems. It includes a review of logistics development, the characters of various transport operations, future direction in logistics development, and its cooperation with transport systems.

The chapter concludes that competition is no longer linked to the importance of maritime artery or its infrastructure but the services offered by this artery. Finally, it suggests that the countries located on the Red Sea must cooperate to move toward integration and service complementarities and avoid competition and/or loss of opportunities. The pressing strategic question of "can we achieve integration and complementarities between the ports of the Red sea" needs to be dealt with without delay. The alternative can lead to unbalance in the economy and finance of the planned megaprojects and threatening their profitability caused by force of circumstance competition which is in full swing.

Keywords Maritime transport • Red Sea • Suez Canal Regional Development Project • Piracy • Robustness and resilience • Disaster management • Logistics • Ports overcapacity • Environmental and sustainability issues • Alternative sea routes

H.H. Abbas (✉)
President, EHAF Consulting Engineers, Cairo, Egypt
e-mail: habbas@ehaf.com

A.E.H.O. Abd El Halim
Civil and Environmental Engineering Department, Carlton University, Ottawa, ON, Canada
e-mail: a_halim@carlton.ca

A.R. Thomas, S. Vaduva (eds.), *Global Supply Chain Security*,
DOI 10.1007/978-1-4939-2178-2_10

Introduction

World trade grew at an accelerated pace throughout the twentieth century. The emergence of a vibrant trading bloc in the Eastern Asia has gradually become the most characteristic element of the business scenario of the world since the mid-1970s International Transport Forum (2009). During the last decade of the twentieth century, China has become the expansion axis of world trade. Currently, more than 90 % by volume of international trade is by sea (Fig. 1). For 200 years, the classic route from the ports of the North Sea crosses the Mediterranean and then the Suez Canal to reach the east of Asian continent. The geographical position of the Suez Canal makes it the shortest route between East and West as compared with the Cape of Good Hope. The unique geographical position of the Suez Canal makes it of strategic importance to the world and to Egypt as well. The canal provides the shortest distance between East and West which results in important benefits to trading nations. In addition to savings in travelled distance and time, the trips across the Canal save fuel, shipping operation costs, and a safer and more secure path. As world economies become ever more globalized and interlinked, international logistics and maritime (shipping and ports) industries are experiencing challenges as well as enjoying greater business opportunities.

Subsequently, Egyptian transport planners and business managers have been busy for years trying to mobilize the nation resources for the project development of the economic zone of the Suez Canal region. A project that aims to create an industrial and logistical spine and is expected to become the main axis of the Suez Canal area. Similarly, Djibouti for its part seeks to deepen its relations with other major regional and international ports. Saudi Arabia on its side of the Red Sea is also modernizing its maritime infrastructure of the port of Jeddah.

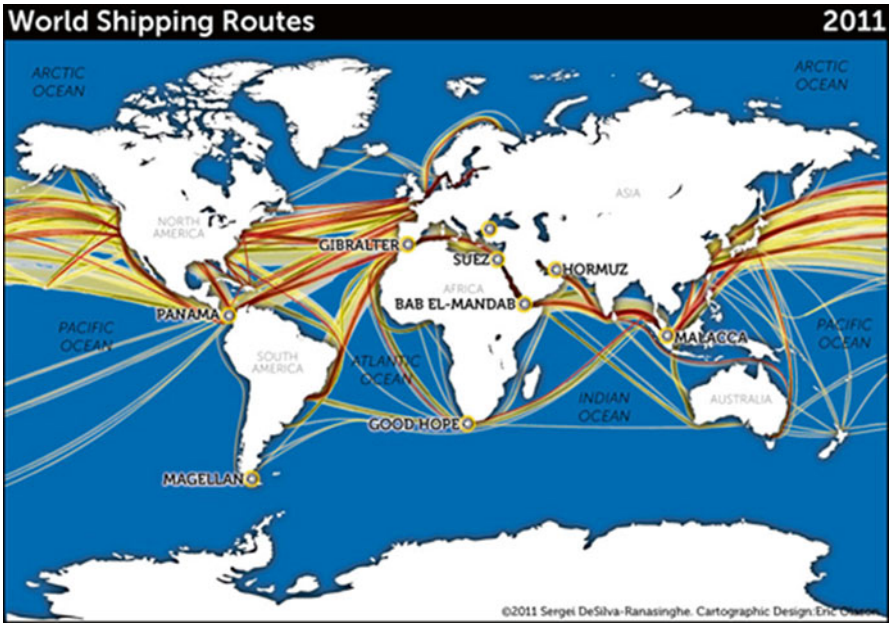


Fig. 1 The Global Shipping Routes (Ref. MSC newsletter)

It is therefore legitimate to ask whether this momentum should take into account the challenges and the current international situation posed by the acts of sea piracy. The terror of piracy can cause shipping authorities and insurance companies to consider other alternative sea routes (far north), competition with existing modern maritime infrastructure in the region (Dubai, Oman) or even land transport such as pipelines and trains. The challenges facing Egyptian planners have become more apparent after the January 25th revolution and the fears associated with eventual closure of the Suez Canal.

Mega Maritimes Projects in the Red Sea

Competition for taking control of the Red Sea or pick up the trade that uses this path existed since antiquity. Today the ports of many countries have experienced a remarkable development that includes the ports of the East Africa region and the Middle East: Sudan, Eritrea, Djibouti, Kenya, Tanzania, Saudi Arabia, Yemen, Oman, and the United Arab Emirates (Fig. 2); many of these nations invested great

Fig. 2 The Red Sea (Ref. http://www.worldatlas.com/aatlas/infopage/redsea.htm)

sums of moneys and effort to redesign and build old and new ports. They have experienced numerous development activities reflecting the value of their strategic locations on the shores of a sea route that is among the busiest in the Red Sea and the Indian Ocean. All these ports are expecting to become the regional hub of shipping and the front door of trading excellence.

Among these ports is the container terminal of the Port of Aden ACT which until 2012 was run by DP World of Dubai. DP World helped to increase Aden's port capacity from 700,000 containers per year to 1.5 million in 2012. The container terminal is the largest in Yemen. It has two quay platforms each 350 m long with 18 m depth mooring side and a hinterland of 43 ha. It allows berthing of vessels and containers day and night, 7 days a week. Also it is noted that the Yemeni authorities have launched an ambitious project of LNG through the discovery of large reserves of natural gas in the country. Dubai ports DP World is a part of DP World's International network, the Emirati marine terminal operator. The company's base is in Dubai and is one of the largest marine terminal operators in the world. The company operates more than 60 terminals across six continents, with container handling facilities generating around 80 % of its revenue.

One shall not forget Jeddah Islamic Port JIP which is the largest Saudi port and one of the largest in the Red Sea, thanks to the gigantic port infrastructure. JIP has treated more than 7 million containers and nearly 130 million tons of goods in 2012. In addition to JIP, other Saudi ports represent a potential threat to all ports of the Red Sea. These Saudi ports are modern and sustainable because they enjoy among other things, a promising operational efficiency and optimal movement of cargo.

It is important to consider the port of Djibouti which is a key regional hub of shipping and a gateway to the East Africa. The country has a long coastline of 370 km. The construction of the port of Djibouti in 1906 came just after the removal of the French colonial administration. The republic of Djibouti is located at the southern entrance to the Red Sea and enjoys a privileged geostrategic position at the crossroads of major international maritime routes and busiest shipping lanes (Abbas 2013).

International Market Evolution of Maritimes Transport

Shipping has always been and remains the most economic mode of transportation of most heavy goods over long distances. Maritime industry plays an important role in international freight. It provides a cheap, safe, and high carrying capacity conveyance for consumers. Therefore, it has a vital role and significant position in the transportation of bulk goods, such as crude oil and grains. Its disadvantage is its longer transport time, and its schedule is strongly affected by weather factors. Geographic distances not only increase transportation costs but also complicate decisions because of inventory cost trade-offs resulting from increased lead time in the supply chain. Ports are essential in transport logistics. However, to improve the performance of their ports, many countries in the region have undertaken reforms and invested heavily in order to cope with the evolution of maritime transport and

Fig. 3 The trade routes through the Suez Canal (Ref. http://www.suezcanal.gov.eg/sc.aspx?show=10)

attract a demanding clientele. The press release 2013 of the WTO Secretariats revealed that in the last two decades, the total value of global trade has increased by approximately US$ 20 trillion. This has led to innovate in logistics and supply chain for the purpose of cost reduction of shipping goods and services across borders, time saving, mistake reduction, and increasing productivity. In addition, with the increasing piracy acts by gangs and terrorists in the southern entrance of the red sea, more demands were placed on naval presence of several European, Asian, and American nations. These challenges while increase the cost associated with sea shipping progress and developments continue to be seen in the region.

Nearly 10 % of world trade and 22 % of containers are passing through the Suez Canal (Fig. 3). Geographical and nautical Suez assets are conducive to the reception of large ships that bring more traffic in the Mediterranean and will capture a maritime traffic growth potential from Asia via the Suez Canal. Containers have had a profound impact on supply chains and national economies. There is no doubt that containers make the process standardized and streamlined. Also shipping containers have made shipping less labor intensive and more dependent on automation which result in a lot cheaper loading and unloading operations which should make longer supply chains more affordable. One important advantage of the containers operation is the significant savings in the time invested on ports.

In a set of 22 industrialized countries, containerization explains a 320 % rise in bilateral trade over the first 5 years after adoption and 720 % over 20 years. By comparison, a bilateral free-trade agreement raises trade by only 45 % over 20 years and GATT membership adds 285 %.

All shipping sectors have been affected by the slowdown in the global economy in 2012. In 2013 first half results remain a concern for both the container transport sector than for other sectors of shipping. The countries concerned are called to reflect the slowdown in the definition of strategies of port and maritime development

in the medium and long term. A business partnership is needed between the countries of the Red Sea, especially since they all share a common goal and they serve customers requiring the same needs.

The risk is great to see a port appear overcapacity at the regional level of the Red Sea. Moreover, the risk of overcapacity could open a risk of dumping transport. Competition resulting in an even greater reduction in costs and collapsing rates of using infrastructure and equipment make them difficult to amortization and tough for ports to cover their high fixed costs and operating expenses.

Logistics and Supply Chain

Maritime transport (shipping and ports) is concerned with the movement of goods and/or passengers between two seaports by sea. Global supply chains and transport networks form the backbone of the global economy, trade, consumption, and economic growth. Similar to all transportation modes, ports in the transport chain cannot be understated since all goods and passengers transported by sea require an origin and destination or the use of at least two ports. Logistics and supply chain management relates to the coordinated management of the various functions and activities responsible for the flow and transformation of raw materials from suppliers into final product through a number of operations within an organization and then reaching out to its customers. Maritime logistics is attributed to the physical integration of transport modes and the evolving demands of end users. The application of information technology (IT) within the supply chains has increased dramatically leading to much improved communication and better services.

Companies are increasingly organizing production of goods and services through global supply chains. Products are processed, and value is added in many different countries. A company's ability to participate in these chains depends greatly on their government's policy choices: the extent of restrictions on market access, the efficiency of border management, information technology capabilities, transport and logistics services infrastructure, and the business environment. Even if tariffs on their exported goods are zero, firms that confront high and uncertain border costs and inefficient and unpredictable logistics will not be able to compete with firms in countries that provide a more efficient economic and better business environment (Analysis of the economic situation 2012; Analyse de la Conjoncture Economique 2012). Many different policies and administrative procedures can artificially break the supply chain by introducing discontinuity and affecting reliability.

Supply chain security refers to efforts that will enhance the security of the supply chain, the transport, and logistics system of the world's cargo. It combines traditional practices of supply chain management with the security requirements driven by the threats such as terrorism, piracy, and theft (Dornier and Fender 2007). A number of regulations and voluntary programs have been implemented throughout the supply chain to improve the security of cargo moving internationally. Delivery reliability is the main key strategic attribute in supply chain management. It is essential to establish a reliable supply chain to achieve the liberalization and

facilitation of transport trade and services and to enhance safety, security, and efficiency and to achieve environment-friendly transportation systems.

Modern transport logistics can be understood as the integration of goods flow and information in a supply chain. According to the European Logistics Association, the logistics costs in relation to annual turnover can amount to more than 30 % in the food industry, 27 % in the metal industry, and 15 % in the automotive sector.

In conclusion, logistics and transportation have some relevance, they have interdependent relationships that logistics management needs transportation to perform its activities, and meanwhile a successful logistics system could help to perform environment and transportation development. Without the link of transportation, a powerful logistics strategy cannot bring its capacity into use of its full potential. The supply chain structures should be adaptable and agile so that they can quickly adjust and respond to the market and economic conditions.

Environmental Sustainability

Two important factors affecting the global supply chain, one concerns the environmental and sustainability issues; the other is the resilience. The truck fuel consumption and the CO_2 emissions from freight transport should be critically managed. The objective of limiting the energy footprint and controlling the global problem of global warming and the emission of greenhouse gases cannot be neglected. It is essential to strengthen and promote the need for cleaner energy sources for suitable development and green growth in the port and shipping industry (Annual Work plans 2013). Also it is necessary to indentify solutions and best practices regionally to prevent and reduce harmful exhaust emissions from international shipping in the region for the protection of the marine and atmospheric environment.

Also reducing fuel consumption will result in public health benefit and reduce the damage from natural disasters that are related to climate change. Reduced fuel use will also have a positive impact on air quality. Also, slow streaming has significant environmental benefits. Speed limits in the shipping sector has been reduced in response to an increasing supply of ships, a slower increase in demand for maritime transport, and rising fuel prices. Consequently, the emissions of carbon and sulfur dioxides are reduced in line with the energy consumption. The legal feasibility of regulating ship speed depends on where and how the speed control is imposed. However, a coastal state and ports authorities can impose slow steaming on all ships as condition for entry into its ports.

Supply Chain Resilience

The world trade is completely dependent on maritime transportation systems, but these systems are vulnerable toward disruptions. The consequences when the transportation system should break down are serious. Therefore, it is important to

provide the system with the ability to restore and to continue its function and mission to move goods after a disruption has occurred. Disruptions are bound to occur; it is critical to address questions such as: how the systems may be prepared to cope with these events, and how can we increase the robustness and resilience of the system to improve response and rapid recovery of economies struck by disasters. Resilience is thus regarded as an advanced phase in the evolution of traditional place-centric enterprise structures to highly virtualized customer-centric structures that enable people to work anytime, anywhere. Resilient supply networks should align its strategy and operations to adapt to risk that affect its capacity. Resilience is a necessity as risks are not forecast-able by traditional means.

IT can provide significant resilience gains through four main channels: analytics, data information sharing, scenario modeling, and preprogrammed responses.

Suez Canal Regional Development Project

Egypt is positioned to become one of the nations to gain the most and to prosper in the emerging global economy. It is important to put in place the infrastructure and logistics systems that will enable Egypt to play a real role as an African hub point of entry and exit for trade between Asia, the Middle East, and Europe in the dominant directions from south to north where oil and gas transit (Presentation of Suez Canal Corridor Development Project 2013). The geographical position of the Suez Canal makes it the shortest and safest route between East and West as compared with the Cape of Good Hope, in addition of being an important military route (Fig. 4).

Fig. 4 Aircraft carrier USS Nimitz passes under the friendship bridge during a transit of the Suez Canal (Ref. Handout photo provided by the U.S. Navy, taken on Oct. 20, 2013. REUTERS/U.S. Navy/Mass Communication Specialist 3rd Class Billy/Handout)

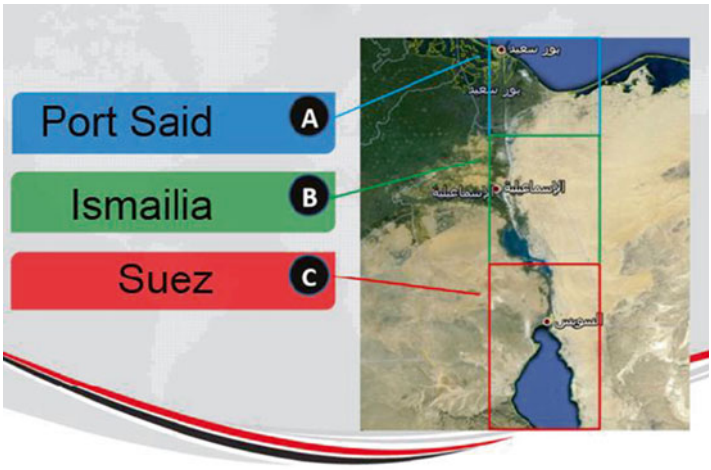


Fig. 5 The Suez Canal proposed strategic hub for logistics and maritime transport (Ref. http://weekly.ahram.org.eg/News/3153/-/-.aspx)

The Canal route achieves saving in distance which is translated into other saving in time, fuel consumption, and ship operating costs and sizeable reduction in CO_2 emissions. In addition, it is considered the safest in terms of climatic conditions and security threats. The Suez Canal and its surrounding land shall become a strategic hub for logistics and maritime transport on an area of 7,000 km, including Suez, Port Said, Ismailia, and North and South Sinai. The project is planned to be completed before 2017.

Suez and Panama canals are the two main artificial channels created by man and used for global maritime traffic. They each bear the signature of the same French diplomat and entrepreneur Ferdinand de Lesseps. The Suez Canal is a project located in Egypt, long of 193.3 km, wide 280–345 m, and deep 22.50 m. In the north, it connects the city port of Port Said on the Mediterranean Sea with the city of Suez on the Gulf of Suez at its south (Suez Canal Authority 2012). The development of the Suez Canal is an integral regional project (Fig. 5), a project which has not ceased to bubble. By providing a gateway between Asia and Europe, the Suez Canal plays a strategic role in the history of international trade.

The door of the Suez Canal is a strategic trade corridor that must acquire the necessary capacity to accommodate increasing volumes of goods shipped to and from Asia and Europe. This involves the creation of several industrial and storage regions between Port Said to the north and south of Suez port. These regions are known as ZIP which possesses many docks and can accommodate large boats and various types of goods and dealing with many modern factories and refineries. The main areas include the northern Gateway (Port Said East, the industrial zone, Port Said West, and Arish Port) and the southern Gateway (Adabiya Port, Sokhna Port, and the special economic zones in the area at the northwest of the Suez Gulf).

The Suez Canal development project should be a strong part in the world supply chain and expected to contribute significantly to world trade and goods transported by sea. The project is expected to achieve the following objectives:

- Export and international trade development
- Creating new centers of growth in the region through diversification and expansion of existing activities
- Ensuring long-term economic growth and attracting foreign investment
- Job creation by implementing labor-intensive projects
- Increased volumes of cargo transport
- Increased share of logistics value added services
- Higher share of multimodal operations
- Improving the regional balance by providing economic and investment opportunities for the population in Sinai and making it attractive for national and foreign investments

Egypt will go through four stages to develop each port in the region:

1. Build container and multipurpose terminals, where vessels can unload their freight for temporary storage.
2. Establish distribution centers, where oil and cars will be primarily stored and picked up by other vessels for distribution (petroleum terminal – roll-on and roll-off term).
3. Construct a bunkering terminal, logistics, and service centers in all terminals.
4. Build industrial hubs and logistics centers around the Suez Canal, in order to take in containers and manufacture goods.

To this end, the Government of Egypt has announced its intention to develop the Suez Canal area along the Suez Canal waterway, transforming it into an international logistics center and a global hub to ensure the long-term growth of the Egyptian economy (Fig. 6). The project focuses on two gateways and Ismailia midway area: Sharq Al Tafriaa east of the city of Port Said, the valley of the technology in Ismailia, and an industrial area northwest of the Gulf of Suez.

The multi-terminal in Port Said is a deep water port aims to attract large vessels around a free industrial zone of 90 km^2 which must accommodate international-level companies.

The Ismailia area must accommodate the valley of technology on the model of Silicon Valley. Ismailia will be focusing on tourism, agriculture, and industry, offering 216 million job opportunities. The government will offer 69 pieces of land for young investors to encourage them to create small- and medium-sized businesses (SMEs) and will help in creating the Technology Valley, a city based on industries in software development and medical technology, including scientific research centers and academies.

Finally, the largest special industrial area of 233 km^2 to be built in partnership is expected to operate in the Gulf of Suez. The Adabiya Port will be expanded to reach 180 % of its original size. It will serve as an example for the other to-be-developed ports. The northwest Gulf of Suez will become a hub for several sectors, such as

Fig. 6 The three developed zones among the Suez Canal (Ref. TML daily newspaper 22th Feb 2011)

tourism, housing, investment, heavy industry, petrochemicals, and trade. The Suez Canal development project will also connect roads on each side of the waterway through nine different bridges and tunnels.

Challenges

Any economic organization faces two basic challenges: first, it must survive the challenges of today, and second, it must adapt to tomorrow's challenges. Therefore, one must examine the issues and challenges of port capacity and its possible impact on the economic development in the Red Sea. In fact, the high costs of port infrastructure projects require a critical review of current expectations concerning the development of trade in goods. Numerous studies that provide a significant increase in global trade made the expected volume of goods the absolute necessity of developing infrastructure. However, in contrast to this forecast, there are pessimistic scenarios which fear that the growth of world trade bows.

The competitiveness and the attractiveness of port cities today depend on various factors: on external variables which are difficult to control such as globalization, the rising cost of energy and raw materials, or regulatory pressure on industrial activities and maritime transport and on internal variables such as governance, port infrastructures, and access to centers of consumption of the hinterland.

A review of Marine Transport warns that supply and demand imbalances are causing shrinking freight markets and reducing opportunities of the finances of

many shipping companies. Subsequently, such a situation tends to lower freight rates, affect earnings, and erode profit gains. The UNCTAD report suggested that the average cost of shipping a 20 ft equivalent unit (TEU) container from Shanghai to Northern Europe fall from $ 1,789 in 2010 to $ 881 in 2011, an unprofitable freight rate for vessels and carriers. This decline of profit affects also ports and is attributed to competition. Customers demand for customized efficient services is continuously increasing. This puts pressure on organizations working in the sea shipping field. The competition is increasing to fulfill high service quality. Meanwhile, due to high competition, services have to be provided putting in mind controlling costs. Current maritime customers care about service quality more than the delivery price.

There are several international plans that are underway seeking to explore new regions for natural resources and/or new sear routes for global trade. The problem with some of these plans and issues, which are listed below, is the lack of serious consideration of the adverse effects or negative impacts on the environment and human health due to the proposed or expected construction of new infrastructure. In addition, the man-made plans will lead to the provision of transport services causing air pollution, the congestion of cities and ports, soil erosion, and the destruction of wildlife and plants. The new plans and issues raise several questions and concerns including:

- Alternative routes and development of the Arctic region by opening the way to the far north linking the Atlantic to the Pacific due to climate warming. A journey of special significance is the Chinese vessel Yong Sheng which has set sail from Dalian in August 2013 to reach Rotterdam in September after a 35-day historic journey through the Arctic's sea route, saving 2 weeks from the traditional itinerary between Asia and Europe via the Suez Canal. The trip raises the challenging question "Will the Northern sea make the Suez route become obsolete?"
- What would be the consequences of a possible reducing the importance of or even the closure of the Suez Canal on countries bordering the Strait of Bab el Mandeb and along the Red Sea: The Canal was closed five times; the last time was the most serious one since it lasted for 8 years due to the Arab-Israeli wars. The closing of the Suez Canal between 1967 and 1975 was a substantial shock to world trade, and the impact of the increase in transportation distance was significant. Can this closure be repeated again, and what if Egypt was forced to close the Suez Canal again? The economic and military effects of the Suez's closure would reverberate throughout Asia and the West.
- The rise of organized piracy especially at the southern entrance to the Red Sea: The southern part of the Red Sea is adjacent to the Somalia coasts, Eritrea, and Gulf of Aden which are becoming heaven sake for piracy and armed robbery. Piracy is considered an international crime, and its repression requires universal jurisdiction. The piracy leads either to divert the ships to the Cape of Good Hope; hence the increase in transport costs due to insurers increased premiums or giving in to the demands of the pirates. In all cases, prime insurance monies are skyrocketing. All the factors leading to piracy are available in Somalia, a political

anarchy, a disintegrated and poor country, armed gangs, fighting groups, and a major shipping route. In the country, the pirates have no trouble to trade the goods in perfect illegality. However, the violation of Somali waters by foreign trawlers led the Somali fishermen to complain about illegal fishing and overfishing by European and Chinese which drive the Somali fishermen to piracy. So far, naval forces of European countries, the USA, and other nations with interests to maintain its trading routes safe and secure challenged the Somali pirates' attempts to shut down Europe's supply chain and trade lines. The question is will the pirates succeed?

- The creation of highly sophisticated and reasonably priced State's owned port facilities around the Arabian Peninsula stretching from Kuwait to Dubai and Oman: the gigantism of these port infrastructures and overcapacity lead to the obvious question: are there really necessary or urgent need to justify the high initial investment and capital costs associated with their establishment? Also, at the same time the plans of creating new and additional port facilities in the Indian Ocean and in the Red Sea are extending. Those large-scale ports are not relying on local or regional populations' requirements but trying to constitute hubs to serve the global market. The danger is that there's no coordination or long-term economic justification for such plans. The key question is how robust demand will be over the next 10 years, and is there a Market for all these transport infrastructure developments?
- Slowing global economic growth: should we expect in the medium term that Asian infrastructure growth and therefore the global trade bow? The world trade growth is likely to be slower, and the economic slowdown in Europe continues to suppress global import demand. When giant's economies will slow down after two decades of rapid growth?
- Uncertainty over future fuel prices: fuel prices have gone through dramatic fluctuations in just the last decade alone, which dramatically changes the economics of maritime and port facilities putting pressure on port tariffs. Uncertainty about oil and gas prices led energy companies to avoid big ticket transactions in 2013 tending toward smaller deals. Why do fuel prices rise and fall? Also, in light of the so-called Arab Spring, will the outcome lead to stable and viable economic and political governments?
- Avoidance of the Mediterranean which would lead many ships to prefer passing through the Cape of Good Hope. Since the widening of the Suez Canal in the 1970s, the Cape of Good Hope has lost some of its strategic importance but still remain an important maritime passage. The Mediterranean Sea is a formidable trade asset which should encourage countries sharing its shores to strive to protect and to maintain it safe and secure. The increase in Mediterranean trade led national authorities to invest in new maritime infrastructures and advanced ports equipment. The burden of these huge investments may carry the risk of the avoidance of Mediterranean ports in order to reduce costs and fees. This situation would of course favor Northern European ports such as Hamburg, Rotterdam, and Antwerp to the detriment of Mediterranean ports.

- Will railway assume a new role in the global trade? Competition that involves the comparative advantage of using rail or maritime transportation is the distance which remains one of the basic choice determinants. Is maritime transportation losing out its competitive advantage over other modes of transportation like railways or still retains its competitive edge over other transport modes?
- Economic cycles are part of human history, and a weakening of the economic capacity of some countries such as China and India should be expected. China ordered more than 1,400 companies in 19 industries to cut excess production capacity, part of efforts to reshape the country's economy and to shift toward slower, more sustainable economic growth. In India, the lower growth together with high inflation persistence could weaken the country's debt profile and raise financing costs.
- Approximation of wages in China and attempts to increasing them to the level practiced in the West due to the strengthening of the middle class and increasing of its purchasing power could have adverse effects. China and India based their competitive advantage in large part on lower production costs. Over time, they will shrug off these low-cost origins and will become known for innovation and premium products as did the companies of Japan and Korea. Many countries in Asia have seen a rapid rise in wages since the late 2005 and that causes an increase of the production costs. This would mean that manufacturing in China or India will not be the cheapest place anymore, and businesses will face pressure on their profit margins to maintain their competitive advantage over the West. These changes lead to the question of how they would affect the movement toward new ports.

Developing Port Competitiveness

Port developments continue throughout the world at an uneven pace spurred on by national needs to import and export and a chance to seize a share of growing world seaborne trade through trans-shipment opportunities. Countries with access on the Red Sea can apply a wide range of policies that aim at increasing the operational and administrative efficiency of their port networks. This includes decisions on the legal and institutional framework, the selection of an ownership model, or the allocation of funds for infrastructure investments.

The reform should target all entities having a relevant role in the port, such as the landlord, regulator, operator, marketer, and cargo handler, thus reducing port charges and the overhead related to each function. However, considering that port charges only constitute about 8–10 % of the total freight rate from origin to destination in the logistics chain, the lever of reducing port charges appears to be limited as reduction of port handling charges by 50 % would only lead to a total freight rate reduction of 5 % (Proceeding of the International Maritime Transport and Logistics Conference 2014).

To remain competitive in the market and to keep up with trading pace, ports have to be efficient, reliable, secure, and safe in providing services to their customers.

If the safety level is low in a port, incident and accidents are happening more often. Ports should hence take several measures to the frequency and consequences of port accidents. An increase of the safety level at ports would be in the interest of all actors in the supply chain management including ports themselves. Of course security is becoming a major concern in recent years especially when sea shipping is concerned. Regulations, security arrangements, intelligence on information exchange, and effective monitoring and cooperation between concerned parties increase the safe and secure shipping transportation across seas and oceans.

Disaster Management

To effectively manage disasters and transport risks, greater collaboration focus is needed. The success of the infrastructure management is the ability to estimate threats and identify risks then to evaluate these risks and their vulnerabilities. Measures are employed by port facilities and other local marine organizations to protect against seizure, sabotage, piracy, pilferage, annoyance, or unexpected surprise. Considering the costs and complexity associated with increasing maritime security, it is expected that efforts will be made to reduce such costs by means of new technologies in the fields of information and communications, monitoring, prevention, and forecasting. The goal is not only to predict what or when but also to be prepared and able to respond in an informed and planned manner to minimize the impact of a disaster. It is a therefore important to understand and follow security protocols and guidelines which can be summarized as follows:

- Enhance disaster management mechanisms by establishing common standards for emergency and early warning system in cross-border transportation.
- Continue efforts to secure trade and travel by supporting deeper cooperation and developing the capacity required to implement a common security code for all port facilities of the red sea through transfer of knowledge, lessons learned, and best practices to make commerce more secure, safe, efficient, and resilience.
- Exchange information on both government-to-government and government-to-private sector to come out with effective decisions.
- Conduct training courses designed to cover various aspects of maritime practices to provide staff in maritime-related authorities with practical exposure to complex issues of international shipping policies and other related maritime policies.

Toward a Red Sea Maritime Space Without Barriers

To preserve commercial competitiveness in an environment where trade barriers are reduced, the countries of the Red Sea must work together to trade facilitation and simplification of procedures in short time. This will improve the efficiency and

competitiveness of intra-Red Sea maritime transport. It will make in addition the procedures for maritime transport as simple as those for other modes of transport which benefit more from the market. The measures listed below are highly recommended:

- Establish institutional mechanisms and strengthen existing ones to find appropriate solutions.
- Simplify customs and port reporting formalities through the general use of electronic means for the transmission of information and the rationalization of reporting formalities.
- Establish plans or accelerate the existing ones to create a national electronic single window line with international standards.
- Define a harmonized regional framework for the electronic exchange of data and documents trade.
- Facilitate transit through plans trade facilitation
- Encourage the development of infrastructure and logistics services for trade.
- Introduce the e-maritime technologies

Efficiency of Logistics Measures of a Country

Several strategies that a port can adopt to attract carriers and face competition:

- A strategy of differentiation may be based on an advantageous tariff policy for operators.
- A strategy of specialization implies that the port is positioned on a particular segment.
- A strategy of diversification is to reorient its development plan to other sectors.
- An innovation strategy to undertake a completely new activity.
- A strategy based on the cost by minimizing the maximum expenditure.

In fact, a huge value will be added to the national economy of the country where logistics projects would be established to meet the following performance measures which serve as indicative of efficiency of port infrastructure in the country:

- Efficiency of the clearance process
- Quality of transport infrastructure and trade
- Easy to organize deliveries at competitive prices
- Competence of the logistics and quality of logistics services
- Ability to track and trace shipments
- The speed of delivery of the consignment
- Higher levels of security and protection throughout the port

How to Become Partners Not Competitors?

All shipping sectors have been affected by the slowdown in the global economy in 2012. In 2013 first half results remain a concern for both the container transport sector than for other sectors of shipping. The countries concerned are called to reflect the slowdown in the definition of strategies of port and maritime development in the medium and long term. A business partnership is needed between the countries of the Red Sea, especially since our goal is common and that our customers have the same needs.

The risk is great to see a port appear overcapacity at the regional level of the Red Sea. Moreover, the risk of overcapacity could open a risk of dumping transport. Competition resulting in an even greater reduction in costs of using infrastructure and equipment make them difficult to amortization.

Establish a balanced partnership can only be achieved by going to greater coordination between the countries of the Red Sea. This implies among other sharing information and data, the use of compatible and interoperable IT systems, improving coordination and cooperation between all sectors of maritime countries.

Summary and Conclusions

Maritime transport is the backbone of international trade and the global economy. Around 80 % of global trade by volume and over 70 % of global trade by value are carried by sea and are handled by ports worldwide. Given this growth in world trade, there is increasing need for market proximity and responsiveness supply chain. Due to the significant role of the Suez Canal in global trade and the world search for safer and secure sea routes, the mandate of Egypt to take advantage of this asset has never been stronger. Important elements that emerge from this Chapter are:

- It is up to governments to work with great care between themselves and with their partners in the private sector and foreign investors to fully understand the opportunities available in their respective countries in terms of trade, transport, and geography.
- Despite the passage of time, competition between ports in the region exists and will continue to be in the near future.
- Possible impacts of overcapacity in the Red Sea ports could be significant which call for more cooperation and communications between the concerned countries.
- The race for port infrastructure new constructions involving huge investment is a double-edged sword.
- Security and safety of maritime routes and ports will be a major concern in determining future logistics chain. Service providers such as ports and hubs must cooperate with service users, e.g., shippers and trading parties to eliminate the threat of sea piracy and ensure the security of sea transport.

References

Abbas H (2013) Les Infrastructures Maritimes en Mer Rouge: Complémentarité ou Concurrence? Paper presented in French at the colloque Stratégie Logistique et de Transport au Service du Développement, université de Djibouti, Djibouti, 15 and 16 décembre 2013

Analyse de la Conjoncture Economique: Le Transport Maritime, (1er Semestre 2012), Direction Générale des Infrastructures, des Transports et de la Mer- France

Analysis of the economic situation: the Maritime Transport (1st semester 2012), Directorate General for Infrastructure, Transport and Sea-France

Annual Work plans 2013- APEC, Transportation Working Group in Response to Leaders/Ministers/ SOM/SCE Priorities and Decisions, and to ABAC recommendations. (http://www.apec-tptwg.org.cn/new/Transportation%20Working%20Group/annual%20workplans/2013%20Annual%20Workplan%20for%20the%20Transportation%20Working%20Group%20(TPTWG).doc.)

Dornier P, Fender M (2007) la Logistique Globale et le Supply Chain Management. Eyrolles, Paris

International Transport Forum, CEMT (2009) Evolution des Transports (1970–2007)

Presentation of Suez Canal Corridor Development Project (SCC), Cairo International Convention Center, Nasr City, May 2013

Proceeding of the International Maritime Transport and Logistics Conference (MARLOG 3) Logistics industry in the Arab world: threats and opportunities, Alexandria, 09–11 Mar 2014

Suez Canal Authority, Information about the Canal (2012)

Planned and Emergent Strategy

Wade R. Rose and Steven A. Murphy

Abstract Since the 1970s, there has been an ongoing debate in the literature as to the most effective means of formulating strategy. One camp has touted the merits of formal, deliberate strategic planning, while the other camp has maintained that strategy simply emerges over time as a firm takes various actions in response to environmental stimuli. Recently, researchers have recognized the more realistic view that deliberately planned strategies transform during implementation through an emergent strategy formation process. This chapter will review the literature on deliberate and emergent strategies, exploring the perspectives of the proponents and critics from each academic camp. It will then examine the two perspectives as ends of a continuum, citing a number of strategy types that exist between the end points. The concept of planned emergence, or a complementary deliberate and emergent approach, will next be discussed followed by an examination of the numerous empirical studies that have sought a link between formal strategic planning and organizational performance. Finally, a discussion of the emergent impact of chaotic systems and improvisation on deliberate strategy will be followed by perspectives on the future of strategy creation and implementation.

Keywords Deliberate strategy • Emergent strategy • Strategic planning • Planned emergence • Strategy formulation • Strategy creation • Strategy implementation • Chaotic systems • Strategy improvisation • Planning versus performance

W.R. Rose, Ph.D. (✉)
Management of stratergy, Sprott School of Business, Carleton University,
1125 Colonel By Drive, Ottawa, ON K1S 5B6, Canada
e-mail: wade.rose@carleton.ca

S.A. Murphy, Ph.D.
Entrepreneurship and strategy, Ted Rogers School of Management,
Ryerson University, 350 Victoria St., Toronto, ON M5B 2K3, Canada
e-mail: murphy@ryerson.ca

A.R. Thomas, S. Vaduva (eds.), *Global Supply Chain Security*,
DOI 10.1007/978-1-4939-2178-2_11

Introduction

The strategy literature is divided on a number of key issues that are critical to the understanding of this field of academic investigation. Central to the debate is the question of how strategy is most effectively formulated, a topic that has been vociferously contested since the 1970s.[1] While much has been written about the planned and emergent schools of strategy formulation, strategy researchers have not yet reached agreement on their relative merits.[2] As a means of providing empirical support to one side of the debate or the other, numerous studies[3] have tried to quantify the proposed link between strategic planning (i.e., planned strategy) and organizational performance. The results have been mixed.

Deliberate and emergent strategy formation processes have been described as science versus art[4] and as opposite ends of a continuum along which the actual strategy-making techniques of real firms lie.[5] "The strategy maker may formulate his strategy through a conscious process before he makes specific decisions; or strategy may form gradually as he makes decisions one by one. In the first case, the strategy determines subsequent decisions …; in the second, decisions converge into a strategy."[6] Although it would seem reasonable to view a situation-dependent mix of these two poles as providing an optimal solution for companies, there has been an ongoing debate between the proponents of each process. As the debate has evolved, the "vivid caricatures presented by each side of the other's conceptualizations of strategy making bear little resemblance to the realities of strategic planning as pursued by large companies."[7]

> To describe these as competing perspectives would be an understatement – Mintzberg (1990), for example, ascribes failures as diverse as the Vietnam War and the collapse of Bendix to the design school (grand strategy). Alternatively, the incrementalist school has been dismissed as 'a Shirley McLaine world of New Age mysticism in which rationality is devalued' (Grant 1995, p 21). … However, the bulk of empirical strategy research, and the views of most practitioners (Ginter et al. 1985) remain more closely aligned with the grand strategy school.[8]

These two disparate views of how strategy is formulated are discussed below.

---

[1] Andrews (1971), Ansoff (1991), Mintzberg (1977), Mintzberg and Waters (1985).

[2] Boyd (1991), Brews and Hunt (1999), Greenley (1994), Holloway (2004), Miller and Cardinal (1994), Schäffer and Willauer (2003).

[3] Falshaw et al. (2006), Hopkins and Hopkins (1997), Thune and House (1970).

[4] Parnell and Lester (2003).

[5] Boyd and Reuning-Elliot (1998), Mintzberg and Waters (1985).

[6] Mintzberg (1977), p 29.

[7] Grant (2003).

[8] Mintzberg (1990), Grant (1995), Ginter et al. (1985), Boyd and Reuning-Elliot (1998).

Planned/Deliberate Strategy

A 2003 Bain survey of US and European firms reported that 89 % employed a strategic planning process.[9] Strategic planning refers to a deliberate analysis and planning approach designed to create a strategic plan that would be used to guide the actions of the firm over an upcoming period. Typically, an internal analysis is carried out to identify the organization's strengths, weaknesses, and competencies. An external analysis focuses on opportunities and threats brought about by the current and projected conditions in the market including global, national, economic, customer, competitor, supplier, distributor, and partner factors, as well as pertinent factors relative to changes in technology. Strategies are devised to address the internal and external situations in ways that maximize the possibility of success for an organization. These strategies are evaluated by senior management, and the preferred strategy is chosen and implementation follows. The choice may be mediated by managerial values and issues of social responsibility.[10]

A deliberate strategy formation methodology is characterized as a planning system with some level of formality whose aim is to devise and implement a plan that will realize the intentions of the organization's leadership.[11] To be perfectly deliberate, the process must fulfill three criteria: the organization must have precise intentions and have communicated them in detail; the intentions must be common to all components of the organization; and the intentions must have been fulfilled exactly as intended without interference from the environment.[12] This insinuates that the organization must have perfectly predicted the environment or have been in control of the environment. By this definition, no process is perfectly deliberate as no organization can perfectly predict the environment.

Mintzberg is quite critical of formal strategic planning, noting that it "repeats itself so often and so mechanically that it desensitizes the organization to real change" and that it "must be recognized for what it is: a means, not to create strategy, but to program a strategy already created."[13] He further states, "show me managers who think they can rely on formal planning to create their strategies, and I'll show you managers who lack intimate knowledge of their businesses or the creativity to do something with it."[14] Mintzberg emphatically states that environmental prediction is not possible and that the strategy-making process cannot be formalized into traditional analyses such as the strengths, weaknesses, opportunities, and threats (SWOT) framework. However, the ability to predict during planning is not necessarily a precondition of control during strategy implementation.[15]

---

[9] Bain and Co. (2003).

[10] Ansoff (1991), Mintzberg (1990).

[11] Ansoff (1991).

[12] Mintzberg (1977), p 29.

[13] Mintzberg (1987).

[14] Mintzberg (1987), p 74.

[15] Wiltbank et al. (2006).

Given the results of the Bain[16] survey and Ansoff's[17] perspective on industry's heavy reliance on formal strategic planning as its preferred strategy formation methodology, Mintzberg's[18] position seems extreme. Bain's[19] survey demonstrates that deliberate strategy formation is used across industry; it is reasonable to assume that managers feel it is a profitable use of resources or the resources would be deployed in some other way. However, the emergent strategy formation methodology also has its proponents.

Emergent Strategy

To be perfectly emergent, Mintzberg and Waters[20] state that a strategy must lead to consistent action over a period of time in the absence of intentions by decision makers in the organization. These patterns of action can arise as a result of unconscious tendencies within the organization or by the influence of environmental forces. For example, this process would be present in what Holloway defines as strategically agile organizations, which "are essentially self-organizing systems that progress and succeed through wider use of initiative and self-control with little or no need for intervention from senior management."[21] The process of emergent strategy formation can be seen to a greater or lesser degree in most organizations.[22]

Holloway[23] notes that people "closer to the coalface" are better positioned to make strategic decisions that will achieve business objectives. He cites Entrekin and Court's[24] example of commercial airliners that spend considerable time off their true course during flights yet still achieve their objective of time and place arrival due to the actions of the pilot. However, in this case, Holloway[25] may be confusing strategy with tactics. While commercial airline traffic patterns are governed by strategies with respect to flight levels and headings based upon tradition, efficiency, and safety, the minor weather-, comfort-, and efficiency-related course corrections made by a pilot in flight to stay within the parameters of these strategies are simply tactical actions. Holloway[26] might have been more accurate if he had stated that the tactical actions taken by functional experts in organizations to stay within broad mandated strategies do not require senior management intervention.

[16] Bain and Co. (2003).

[17] Ansoff (1991).

[18] Mintzberg (1987), pp 66–75.

[19] Bain and Co. (2003).

[20] Mintzberg and Waters (1985).

[21] Holloway (2004), p 472.

[22] Grant (2003), pp 491–517, Mintzberg and Waters (1985).

[23] Holloway (2004), pp 469–483.

[24] Entrekin and Court (2001).

[25] Holloway (2004).

[26] Holloway (2004).

Mintzberg[27] states that slowly, over time, a pattern of actions and/or decisions will emerge that will form a strategy. This strategy emergence results from trial and error and resultant feedback loops. While this may often be the case, it could be argued that many firms could not survive this process, especially those without significant financial reserves finding themselves in difficult market cycles. At the very least, trial and error can be an expensive methodology in terms of time and resources.[28] However, Ansoff does allow that emergent strategy formation can be successful in environments where change is incremental and slower than organizational response. He sees this as the case in approximately 20 % of firms in developed economies.[29]

Ansoff[30] argues that making rational choices on possible strategies is especially important in turbulent environments because it focuses the organization on alternatives that are most likely to succeed while saving the effort and time that would have been devoted to alternatives with little hope of success. Mintzberg[31] takes the view that making long-term rational strategic choices is not possible because managers cannot make reliable environmental predictions.

Mintzberg[32] states that one of the benefits of an emergent strategy is that it is not explicitly stated. He feels that explicitly stating a strategy can cause the implementing bureaucracy to build up too much momentum, thereby negating the tendency to ponder its actions. He goes as far as to blame the post-1965 United States (US) military escalation in Vietnam on the explicit nature of President Johnson's strategy. He further cautions that changing an explicit strategy once bureaucratic momentum has formed can be extremely difficult.[33] Rather than condemn explicitly stating strategy, another perspective on this situation might be to emphasize the importance of explicitly stating an effective strategy as opposed to an ineffective strategy. Ansoff notes that explicitly stated strategies need not be inflexible. They can be guidelines that "control erratic deviations from the strategy"[34] while allowing latitude to exploit appropriate opportunities as they arise.

Mintzberg[35] is of the opinion that formal strategic planning leads to mundane strategies, while emergent strategies tend to be more creative and innovative. In a 1987 paper, he refers to the process of strategy formation as *crafting strategy*, using a potter crafting clay as an analogy.[36] Just as the potter may simply wait to see what shape emerges from the clay, Mintzberg[37] makes the point that strategies can simply

[27] Mintzberg (1977).
[28] Ansoff (1991).
[29] Ansoff (1991).
[30] Ansoff (1991).
[31] Mintzberg (1987), pp 66–75.
[32] Mintzberg (1987), pp 28–40.
[33] Mintzberg (1977), p 32.
[34] Ansoff (1991), p 458.
[35] Mintzberg (1977).
[36] Mintzberg (1987), pp 66–75.
[37] Mintzberg (1987), pp 66–75.

form based on the interactions between the firm, its resources, and its environment. While the concept seems valid on the surface, it does not account for the extremely complex internal and external environment in which the firm must operate. While the analogy may be plausible for a company with one or few employees, it is problematic for organizations with hundreds or thousands of actors. A more appropriate analogy for this situation might be a large sailing vessel. While each of the deck hands might have an intelligent perspective as to the tack that the ship should take, when it should change tack, the amount of sail it should deploy, and how these decisions should evolve as the conditions change, if they all acted independently, the ship would be in a state of confusion. While the Captain would be wise to heed the advice of the experienced sailors on board, he/she would be putting the ship in peril if each were permitted to try various actions independently.

Mintzberg uses 3M and Hewlett-Packard as examples of companies where management controls the strategy formation process but leaves the content of the strategies to "people way down in the hierarchy, who are in touch with the situation at hand and have the requisite technical expertise. In a sense, these are organizations peopled with craftsmen, all of whom must be strategists".[38] While ideas are probably solicited from various sources in an organization with a decentralized structure, the strategies are likely decided and controlled by management through the allotment of resources. In practice, it is more likely that similar to other large companies, discretionary dollars spent in areas such as research and development, a key strategy lever, are tightly allotted and controlled by management.

While emergent strategies are important aspects of a firm's total strategy formation process, it may be appropriate to view them as acting within the guidelines developed through a formal strategic planning process. That being said, in situations where unforeseen environmental circumstances have a dramatic impact on a firm, the emergent aspects of strategy may define a whole new direction for a firm. Both methodologies play an important role, are complementary, and may define the end points of a strategy formation continuum.[39]

A Planned to Emergent Strategy Continuum

The definitions presented above for perfectly deliberate and emergent strategy formation processes possess characteristics that make their existence unlikely in a real organization. Regarding these processes as the end points on a continuum, Mintzberg and Waters[40] propose the following eight points along the continuum, starting with the most deliberate and running to the most emergent.

[38] Mintzberg (1987), p 71.

[39] Andersen (2004), Grant (2003), pp 491–517, Harrington et al. (2004), Mintzberg and Waters (1985).

[40] Mintzberg and Waters (1985).

The Planned Strategy This process is characterized by the leadership of the organization deciding on very specific intentions and courses of action, communicating these intentions in a very detailed and precise fashion, and controlling the implementation to ensure compliance. As the strategy is inflexible, success depends upon the ability to effectively predict or control the environment. Mintzberg and Waters[41] cite large mining companies, airlines, and military campaigns as examples of situations where this process is employed due to the necessity to commit significant advance capital resources to the resultant strategy.

The Entrepreneurial Strategy In this case, one leader, often the owner, has control of an organization and imposes his/her vision. The strategy is formulated by this single person and is not communicated other than through the ongoing decisions and direction provided by this individual. Although a predetermined strategy is present, there is also an emergent quality given that the strategy can evolve easily because it is controlled by only one person. This methodology is found in new and/or small organizations where all the members of the organization are willing to follow the precise direction of the leader. It is reasonable to assume that use of an *Entrepreneurial Strategy* style would not be effective in a large organization where many different strategy approaches are likely to emerge, and the majority of participants in the organization have limited contact with the leader.

The Ideological Strategy This differs from the *Entrepreneurial Strategy* in that the vision or ideology is shared by all members of the organization. The ideology is articulated and leads to clearly defined intentions. These intentions are formulated and deeply accepted by the components and actors of the organization and are thus very resistant to emergent change. Religious, charitable, and some nongovernmental agencies can be described as ideological organizations.

The Umbrella Strategy Mintzberg and Waters[42] describe this process as deliberately emergent. The organizational leadership articulates a deliberate vision or set of broad guidelines within which the actors and components of the organization must operate. Within the boundaries or under the *umbrella* of these deliberate guidelines, different strategies are allowed to emerge within different components of the organization. Mintzberg and Waters[43] cite the US National Aeronautics and Space Administration's (NASA) goal of reaching the moon in the 1960s as an example of an *Umbrella Strategy* within which many strategies and approaches emerged from the individual departments and scientists at NASA. Variations of this deliberately emergent approach seem to be used by many multi-division corporations where corporate headquarters provide the *umbrella* and individual strategies emerge within the divisions.

The Process Strategy In this approach, organizational leadership controls the process of strategy formation, and individual components of the organization define the

[41] Mintzberg and Waters (1985).

[42] Mintzberg and Waters (1985).

[43] Mintzberg and Waters (1985).

content of the strategies. For example, multi-division corporate headquarters can dictate the organizational structure, strategic planning processes, and staffing processes and appoint the divisional executives, thereby indirectly controlling the strategy formation process. The design of the system within which strategy is formulated is deliberate, while the strategies of individual divisions are allowed to emerge within the designed system.

The Unconnected Strategies These strategies are formulated by individual persons or components of an organization without guidance or direction from organizational leadership. Mintzberg and Waters[44] use the National Film Board of Canada as an example whereby the individual filmmakers decide their own strategies as to what sort of films they will produce. It should be noted that this methodology is viewed as emergent from the perspective of the Film Board, while it can be viewed as either deliberate or emergent from the perspective of the individual filmmaker depending upon the presence or absence of prior deliberate intentions. *Unconnected Strategies* tend to thrive in organizations such as scientific institutes or hospitals, which house collections of experts facing complex environments. If a particular strategy becomes successful for one individual, it can then migrate to other individuals or to the whole organization as a deliberate strategy.

The Consensus Strategy This process has no deliberate component; it is fundamentally emergent. It occurs when the individuals or components of an organization mutually, without prior intentions, adjust their strategies so that they converge on a particular pattern of actions. This can be an outgrowth of successful *Unconnected Strategies*. Mintzberg and Waters[45] note that it can happen in a quick spontaneous fashion as occurred in the 1950s when the National Film Board of Canada produced its first film for television. Without central direction and in less than a year, 60 % of production effort was for television. This example could also have elements of an *Imposed Strategy* whereby the growth of television in Canada imposed the necessity of making films for television on the filmmakers of the National Film Board of Canada.

The Imposed Strategy These strategies are imposed by the external environment with no prior control or input from within an organization. Environmental forces can include markets, national economic factors, natural disasters, technological advances, or political influences. The strategy formation process is reactionary and sometimes devoid of alternative choices. While totally *Imposed Strategies* are rare, the environment provides some level of influence in most situations (e.g., applicable legislation and laws).

In general, deliberate strategies tend to be formulated through a formal process, articulated in a clear and detailed manner, and controlled through implementation. Emergent strategies tend to arise due to the vagaries of the individuals in the organization and the impacts of the external environment. While the eight waypoints

[44] Mintzberg and Waters (1985).

[45] Mintzberg and Waters (1985).

described above on the deliberate-emergent continuum represent distinct possibilities, it is the interactions between these methodologies that probably appear in most organizations. In what seems at odds from some of Mintzberg's other writings,[46] he and Waters note that "Strategy formation walks on two feet, one deliberate, one emergent… The relative emphasis may shift from time to time but not the requirement to attend to both sides of this phenomenon."[47] This seems to be a more realistic argument given the prevalence of strategic planning in organizations[48] and the inevitable impact that environmental changes can have on these plans. For example, many companies would have had growth plans in place as part of their deliberate strategies during the summer of 2008. The emergence of the global recession would have had a dramatic impact on these strategies as the last quarter of 2008 began to unfold.

Planned Emergence

The long running debate over the relative effectiveness of deliberate versus emergent strategy formation has served to clarify many of the issues surrounding these two methodologies. As discussed above, the proponents of the two perspectives have emphatically stated their cases and disputed each other's views in a series of papers, which have been published over several decades. However, recent studies tend to state the more balanced and realistic view that actual operating organizations must use both deliberate and emergent methodologies in a complementary fashion to strategically manage themselves in an effective manner.[49]

Considering the internal complexity of any large organization and the multitude of external forces impacting it at any given time, it seems reasonable that both deliberate and emergent methodologies have an important and complementary role to play in strategy formation. If an organization did not formally plan and articulate its strategy, at least in broad strokes, the various actors and components of the organization could act independently and without a shared focus. This could lead to confusion, wasted resources, and interactions between actors and organizational components that negatively impact the organization as a whole. Alternatively, if the organization's stated strategy was so rigid that it did not allow the flexibility required to react to changeable external forces, the organization might find itself on a destructive course with no ability to correct itself.

Although Mintzberg's[50] example of a potter crafting objects from clay was used as a metaphor for the emergent strategy formation process, it could be argued that the example more aptly relates to deliberate and emergent processes operating in a

[46] Mintzberg (1977, 1987), pp 66–75.

[47] Mintzberg and Waters (1985), p 271.

[48] Bain and Co. (2003).

[49] Andersen (2004), Grant (2003), pp 491–517, Harrington et al. (2004).

[50] Mintzberg (1987), pp 66–75.

complementary manner. From a deliberate perspective, the potter made a conscious decision at some point in the past to make and sell pottery versus going into another line of work. The potter must have planned the equipment purchases and infrastructure changes (i.e., building a workshop) and allotted the resources to implement the plan. It is also probable that the strategy was explicitly stated to others at some point in time. Inside this deliberate strategy framework, possibly an *Umbrella Strategy*,[51] the emergent strategy formation process takes place as described above.

Perhaps this complementary deliberate and emergent approach can sometimes be one strategy formation process with two parts. In the first part, an organization deliberately plans its strategy given its internal strengths, weaknesses and competencies, and the external opportunities, threats, and competitive forces represented by the environment. This intended strategy is articulated to the organization in enough detail to provide clear guidance to the various actors and components of the organization who will be involved in its implementation. It is often also communicated externally, at least at a high level, to provide signals to external stakeholders. The strategic guidance is structured to provide enough flexibility to allow decision makers to react to environmental changes as they occur throughout the planning period. In part two, the implementation and operation of the strategy is carried out, but the strategy is allowed to transform or evolve as new opportunities, threats, or environmental forces emerge. At the beginning of the next planning cycle, the baseline strategy that is reviewed to judge its effectiveness is the realized strategy that is the product of both the deliberate and emergent aspects of the last cycle. Mintzberg and Waters[52] refer to this as strategic learning.

Although the executives in a particular organization might not describe their process using these same terms, it is clear from the numerous studies in this subject area that a process containing both deliberate and emergent components is used by many organizations.[53] An organization's ability to succeed in meeting its strategic goals may be a function of how well the organization is able to learn from the results of these strategy formation cycles.

Strategy Life Cycles

Mintzberg notes that strategic change is "rather bumpy and ad hoc, with a complex intermingling of periods of continuity, change, flux, limbo, and so on."[54] Based on his 20 studies that include a magazine, an automaker, a government film agency, and the US involvement in the Vietnam War, he proposes that "two main patterns emerge, one superimposed on the other. The first is the life cycle of an overall

[51] Mintzberg and Waters (1985).

[52] Mintzberg and Waters (1985).

[53] Grant (2003), pp 491–517.

[54] Mintzberg (1977), p 36.

strategy – its conception, development, decay, and death. … The second pattern is the cyclical one – periodic waves of change and continuity."[55]

Long periods of stability are interrupted by brief periods of significant change although these stable periods may now be shorter given the accelerated pace of change in the global marketplace. Companies use the periods of stability to fine-tune current strategies, but as a company gradually falls out of alignment with its environment, the need for a new strategy develops. The company reacts to formulate a new strategy in an attempt to re-establish stability.[56] "The real challenge in crafting strategy lies in detecting the subtle discontinuities that may undermine a business in the future. … the trick is to manage within a given strategic orientation most of the time, yet be able to pick out the occasional discontinuity that really matters."[57]

Grove[58] notes that these subtle discontinuities can often signal monumental change despite their sometimes nonthreatening appearance. He refers to them as strategic inflection points and describes them as the eye of a hurricane. Even though all can seem calm, an industry or culture can be on a course that will take it into an environment where much of its current structure may not survive or, at the least, be significantly restructured. Grove[59] cites examples such as the introduction of the personal computer. A more current example might be the introduction of web-based social media, such as Facebook and Twitter. Who could have foreseen their impact on world affairs such as the upheaval in Iran in 2010 or Egypt in 2011? However, even when the need to change is recognized, it is often difficult to achieve. Numerous factors including a strong organizational identity can make it difficult to affect strategic change in an organization.[60]

Miller et al. and Mintzberg note the importance of the interaction between the internal and external environments of an organization; as the organizational and environmental conditions change, so too does the strategy formation approach.[61] Miller et al.[62] depict organizations as entities struggling to maintain equilibrium and stability. Perhaps the key to successful strategy formation is, as Mintzberg[63] suggests, detecting future organization/strategy/environment misalignment before competitors. However, it seems that this would require ongoing deliberate internal and external analysis, and the ability to predict future situations, something that Mintzberg does not support in a number of his writings.

Perhaps it is time to start thinking about strategy as a verb and not a noun. As taught by many business schools and practiced by many organizations, strategy is portrayed as an annual ritual (i.e., noun) whereby an organization's decision makers

[55] Mintzberg (1977), p 36.

[56] Miller et al. (1984).

[57] Mintzberg (1987), p 74.

[58] Grove (1997).

[59] Grove (1997).

[60] Kjaergaard (2009).

[61] Miller et al. (1984), Mintzberg (1987), pp 66–75.

[62] Miller et al. (1984).

[63] Mintzberg (1987), pp 66–75.

meet to examine its internal and external environments and decide the best course of action for the upcoming period. However, these planned strategies are often forced to evolve as unpredictable environmental events, and trends emerge over the implementation period. If some level of strategy evolution is the norm for most organizations, this would imply that strategies are living evolving conceptual entities (i.e., verbs) and strategic plans must be living documents. This is in contrast to the static nature of the documents that are compiled on a once-a-year basis by many firms. In other words, strategies are best conceptualized as verbs because of the changing environments in which they are implemented and the actions that must be taken to help them evolve in a successful fashion. This is accomplished by the monitoring and strategy amending actions of decision makers as an implementation period proceeds.

Planning and Performance: Empirical Evidence

Studies of a possible link between the strategy formation methodology utilized and organizational performance present widely varied results. Some of this disparity may be the result of differing methodologies and a lack of rigor in the execution of the studies.[64] However, the lack of consensus with respect to a link may also be due to the complexity of the relationship and an inability, thus far, to adequately conceptualize the various aspects of the relationship. A number of studies that have sought a link between planning and performance are now discussed.

In an early study of 92 companies, Thune and House[65] found that companies with formal long-range planning consistently outperformed companies using informal planning. The formality of selected companies' planning processes was ascertained through the use of a survey. Performance data consisted of previously published, publicly available financial data over 7–15-year periods (dependent upon the industry). Noting that formal long-range planning is defined as strategic planning in later studies, the authors found that the formal planning companies showed enhanced performance after formal planning was commenced, relative to their states prior to formal planning process implementation.

In a review of 29 studies that specifically investigated the relationship between strategic planning and company performance, Greenley[66] categorized the papers into three groups. Nine of the studies found no relationship between strategic planning (i.e., the creation of an intended strategy) and company performance. The second group had 12 studies that showed evidence of a relationship. The third group contained eight studies that not only showed a relationship, but the authors also claimed and found that companies carrying out formal strategic planning achieved higher levels of performance than those companies that did not. While 20 of the

[64] Greenley (1994).

[65] Thune and House (1970).

[66] Greenley (1994).

29 studies showed some relationship, Greenley[67] concluded that no conclusive relationship could be surmised because of the methodological differences between the studies and a general lack of rigor throughout. He further noted that the methodological differences disallow the possibility of a meta-analysis. Some of the issues noted by Greenley are the lack of a consistent definition for strategic planning; a difference in scope whereby some of the studies looked at strategic planning, whereas others looked at the broader process of strategic management; a variety of performance measures both quantitative and qualitative; different perceptions of what constitutes formality in planning; the different external environments that existed across the companies; the different internal environmental factors that impacted each company; differences in the industries being sampled; and the varied durations of the studies. Without consistency across these issues, it is difficult to compare their results directly. However, this does not invalidate the results of the studies when viewed on an individual basis. It would seem that there is at least some support for a relationship between strategic planning and company performance, given that 20 of the 29 studies provided evidence to support this conclusion.

Brews and Hunt[68] have noted the significant impact that planning duration has on resultant performance. They postulate that it takes at least 4 years for the positive impacts of strategic planning to manifest themselves in a specific firm due to the time required to perfect the process in an organization new to strategic planning. Further, an extended period of time is often required for strategic inputs to reach desired ends. If their suggestions are correct, some of the inconsistent results in planning and performance studies could be explained by the varied experience levels of companies with respect to strategic planning and the possible time lags between implementation and results.

In a meta-analysis of 26 studies, Miller and Cardinal[69] found that strategic planning positively influences the performance of firms. In discussing the mixed results found by numerous researchers, they note that differences in methodology between studies have led to inconsistent findings and the ongoing debate over the value of strategic planning.

Boyd[70] carried out a meta-analysis of 29 studies whose samples totaled 2,496 organizations. Similar to Greenley,[71] he found disparate results with significant measurement errors. He also noted that some results were questionable due to small sample sizes. However, taking a different stance than Greenley, Boyd[72] suggests that widespread numerous measurement problems have resulted in findings that undervalue the actual relationship between planning and organizational performance. He suggests that the benefits of strategic planning are underestimated based on the 29 studies in his meta-analysis.

---

[67] Greenley (1994).

[68] Brews and Hunt (1999).

[69] Miller and Cardinal (1994), p 1649.

[70] Boyd (1991).

[71] Greenley (1994).

[72] Greenley (1994), Boyd (1991).

In a study of 112 banks, Hopkins and Hopkins[73] found that the intensity of the strategic planning effort is directly and positively related to a bank's financial performance. Interestingly, they found the reciprocal also in evidence: greater performance leads to higher levels of strategic planning intensity. This study has an elevated level of credibility because of the large sample size and the fact that the companies were all in the same industry, thereby controlling for some of the external environmental factors.

More recently, Falshaw et al. [74] surveyed 113 companies in the United Kingdom to study whether there was a relationship between formal strategic planning and company performance. However, they did not find evidence of a relationship. They did note that the complexity of the activity, including the many moderating variables, may require a qualitative data gathering approach to allow a better understanding of any possible relationship. This conclusion is significant in that it refers to a general weakness that could be inherent in most of the aforementioned studies. While there have been numerous attempts to find a link between planning and performance, they have been predominantly quantitative. Extrapolating from the comments of Falshaw et al., the inconsistent results may be due to a lack of understanding and theoretical development relative to these two constructs. It has been suggested by several authors that a qualitative approach may provide a more appropriate methodology for theory development and understanding when studying complex relationships and environments.[75]

In reviewing the literature, it becomes apparent that although numerous studies have been carried out involving thousands of companies, there is no consistency in the results from either individual studies, literature reviews, or meta-analyses.[76] Many researchers have stated that the inconsistent results are primarily due to the differing methodologies employed and numerous errors in the execution of the research.[77] Grant notes that "studies relied upon largely superficial characterizations of strategic planning practices based mainly upon questionable data."[78] However, even if more rigor had been applied to more consistent quantitative methodologies, it is questionable whether or not these approaches could adequately characterize such a complex relationship involving a large quantity of dynamic variables in so many firms and industries.

Given the resources expended by a high percentage of firms to carry out strategic planning on an annual basis,[79] the fundamental question of whether or not strategic planning leads to positive, tangible results deserves a credible answer. Because of the high percentage of firms engaged in the activity, one can surmise that industry already implicitly believes in a positive relationship between strategic planning

[73] Hopkins and Hopkins (1997).

[74] Falshaw et al. (2006).

[75] Bradbury and Lichtenstein (2000), Lee et al. (1999).

[76] Schäffer and Willauer (2003).

[77] Greenley (1994), Miller and Cardinal (1994), Boyd and Reuning-Elliot (1998), pp 257–272.

[78] Grant (2003), p 492.

[79] Bain and Co. (2003).

and performance. Although designing a sufficiently rigorous and generally accepted research methodology is a significant challenge, this is an area of academic research that warrants the effort. A possible starting point may be recognizing the inherent complexity of the relationship between strategy formation and performance, and designing study methodologies that reflect the significant number of explicit and tacit factors, and the possible chaotic nature of their relationships.[80] The chaotic nature of the business environment makes the detection of any relationships between the factors much more difficult. However, while these methodologies are unlikely to reflect all of the complex interrelationships inherent in these variables, the resultant research may be a step closer to characterizing the real environment in which strategy is formulated and implemented.

Noting the complexity of the environment defined above, it is understandable that the results of studies simply relating the formality of planning against firm performance can be varied. Numerous variables can affect the planning-performance relationship, and their impacts must be accounted for if a study wishes to truly relate how performance is affected by the various aspects of planning.

Despite numerous individual studies, qualitative analysis of groups of studies, and meta-analyses of selected studies, the literature provides no consensus on the proposed link between planning methodology and subsequent firm performance. A number of researchers point to differing methodologies and a general lack of research rigor to explain the disparity of study results. However, some of the conclusions drawn from qualitative analysis of groups of studies may be too conservative. For example, in his analysis of 29 studies where 20 found a link between planning and performance, Greenley[81] suggests that no relationship can be implied because of the inconsistent methodologies used in the various studies.

Another explanation for the differing results might be the complexity of the relationship between what is planned (i.e., intended strategy) and what is actually implemented (i.e., realized strategy) and in particular, the number of factors that affect the transformation of one to the other. These factors may include characteristics of the organization and the external environment in which the firm operates. Until an enhanced theoretical understanding of strategy formation is attained, it will be extremely difficult to gain any consistent results from planning-performance studies.

Chaos Theory and Chaotic Systems

Chaos has been defined as "the behavior of a system whose final state depends so sensitively on the system's precise initial state that the behavior is in effect unpredictable and cannot be distinguished from a random process, even though it is

[80] Bradbury and Lichtenstein (2000).

[81] Greenley (1994).

strictly determinate in a mathematical sense."[82] Chaos theory is often used to study complex nonlinear dynamic physical systems whose behavior appears random but is in reality a complex set of non-repeating patterns governed by the nonlinear effects of numerous variables and initial conditions. While it is possible to predict the state of the system in the short term, prediction becomes increasingly difficult as the time frame lengthens.[83]

Industries can be thought of as chaotic systems in that they "evolve in a dynamic way over time as a result of complex interactions among firms, government, labor, consumers, financial institutions, and other elements of the environment."[84] This complex list of variables might also include domestic and international economies, suppliers, distribution channels, natural and human-made disasters, technological breakthroughs, management teams, individual executives, and so on. Some of these elements would characterize the specific conditions of an industry or individual firm at an initial state, while others would define impacts at points in the future. As each impact works its way through the system and changes the states of the other elements, a new set of initial conditions, interactions, and states is defined.

Noting the complexity of the system defined above, it is understandable that the results of studies attempting to simplistically relate the formality of planning to firm performance can be varied. Numerous emergent contextual variables can affect the planning-performance relationship, and their impacts must be accounted for if a study wishes to accurately relate how performance is affected by the various aspects of planning.

Whether a strategy is deliberate, emergent, or a combination of both, it is created and implemented in the context of the external and internal environments of the particular organization. External factors such as environmental turbulence and competitive context impact the methodology utilized and the rapidity of the process.[85] The explicit and implicit characteristics of the organization, as well as the characteristics of the individual actors, combine to impact the processes used to formulate and implement strategy. Numerous scholars have highlighted the impact on planning brought about by internal and external context.[86]

The choice of strategy formation methodology and how effectively it is carried out does not occur in a vacuum. It is a consequence of numerous external and internal forces affecting an organization. The accelerating pace of change and the turbulent and extremely competitive environment that exists for many businesses may have resulted in an increasing reliance on a process of "planned emergence" whereby businesses formally plan but retain considerable flexibility to adjust strategies as required to react to their changeable environments.[87] A reasonable approach

[82] S&T Encyclopedia (2007).

[83] Levy (1994).

[84] Levy (1994), p 167.

[85] Grant (2003), pp 491–517.

[86] Ashill et al. (2003), Blythe and Zimmerman (2004), Depperu and Gnan (2006), Harrington et al. (2004), Miller et al. (1998).

[87] Grant (2003), pp 491–517.

may be for organizations to plot a broad path toward objectives while allowing flexibility for course adjustments within set guidelines.

The strategy formation methodology utilized by an organization is also impacted by the internal environment of the organization.[88] Ashill et al. [89] propose an iceberg as a representation of the many explicit and implicit characteristics of organizations that impact the choice of strategy formation methodology. As with an iceberg, the lower non-visible levels, including the organization's underlying values and assumptions, have a significant impact on how strategy is formulated and implemented.

Intended Versus Realized Strategy

Mintzberg and Waters'[90] concept of intended strategy evolving into realized strategy acknowledges the chaotic nature of the environments in which strategy is formed and implemented and the intertwined nature of planned and emergent strategy. In this sense, it is an exploration of "the relationship between leadership plans and intentions and what the organizations actually did. … the label strategy [is used] for both of these phenomena – one called *intended*, the other *realized*."[91] Unrealized strategy is simply the portion of the strategy that is never realized due to various internal and external considerations. The intended strategy is deliberate and can be the result of a planning process or simply the articulated vision of a leader or leaders. This deliberate or intended strategy then interplays with various emergent aspects that come about due to the vagaries of the internal and external environments to form the realized strategy that is actually implemented by the organization. For example, many companies might have had intended strategies in the fall of 2007 that were predicated on continued global economic growth. With the onset of the global recession, these companies would have taken actions that might have been quite different from their originally intended plans due to the emergence of significant external changes in the economic environment. The combination of a firm's originally intended strategy, with the emergent strategies that resulted from its attempts to cope with the economic slowdown, would have resulted in its realized strategy. This realized strategy represents what the firm actually did.

Although the process view of strategy formation recognizes the change from intended to realized strategy,[92] there has not been any rigorous research into identifying and quantifying the factors that bring about the change. To understand how an implemented or realized strategy evolved from the strategy that leadership initially intended to be implemented, one must understand the contextual factors that impact this evolution. For a commercial company, one might surmise that the impacts

[88] Boyd and Reuning-Elliot (1998), pp 257–272, Mintzberg and Lampel (1999).

[89] Ashill et al. (2003).

[90] Mintzberg and Waters (1985).

[91] Mintzberg and Waters (1985), p 257.

[92] Sminia (2009).

would include changes in internal capabilities, competitors' actions, or other changes in the external environment. However, the factors that impact this evolution have thus far not been studied in a rigorous fashion. While the literature contains various researchers' assumptions with respect to what these contextual factors might be, research to identify and quantify these factors is absent from the literature.

Improvisation and Strategy Formation

Our integration of the literature in this chapter has necessarily brought together the camps of planned and emergent strategy. That is, we can reasonably conclude that most firm strategy consists of both planned and emergent aspects. Creating nimble strategy has been a theme in the literature for decades.[93]

One way of describing the required nimbleness of organizations in creating and sustaining strategy has been through the use of improvisation – a form of spontaneous performance. The roots of improvisation work in management arose from improvisation in the fine arts (particularly in theater and jazz).[94] Improvisation has been defined as intuition guiding action in spontaneous ways.[95]

Theatrical improvisation has been applied to the business world for some time.[96] At the heart of such papers is the embrace of paradox. Theatrical improvisation is simultaneously chaotic yet structured, planned (at least usually in the form of a topic or word) yet completely unscripted. Improvisers may plan or practice what they might say or do in a scene, yet they must "go with the flow" once a scene actually begins. In order to do so involves a great deal of mutual trust between improvisers, with an implicit expectation that your partner will provide you with "material" to build upon.

Improvisational theater is sometimes referred to as the art of "yes-and." In this concept, one actor sets the stage for the next actor through a statement or action. The second actor says "yes" to the offer by accepting it and launching in a new direction based upon the opportunities presented by the scene, set, and actors present. In this context, the planned strategy is the initial situation that sets the stage and to which the decision makers say "yes," and the "and" represents the emergent strategies that are taken based upon the opportunities presented by the evolving internal and external environments in which an organization finds itself. Just as there is no way to predict the new directions that an actor might take an improvised scene during its implementation, the same might be said of an extremely creative business leader. The success of the entire scene, for all of the actors on stage (or a firm), is dependent upon some sort of planned strategy (or set of norms) being in place to allow all to improvise in a cohesive fashion.

[93] Porter (1996).

[94] Crossan (1998).

[95] Crossan, and Sorrenti (1997).

[96] Crossan (1998), Moorman and Miner (1998).

The improvisation concept as it applies to strategy is also similar to Mintzberg and Waters'[97] umbrella concept of strategy formation. In theater, the planned umbrella strategy is represented by the set, props, and any pre-decided situation (context) for the scene. The improvisation of the actors is similar to the emergent strategies which are allowed to develop within the bounds set by the overall umbrella strategy.

Paradox can be defined as a statement or a proposition seemingly self-contradictory or absurd but in reality expressing a possible truth.[98] Common examples of paradox include combining the view "he who hesitates is lost" with "look before you leap." In this instance, the notion of planning or preparing seems at odds with the need for decisive action. Yet both of these views can be embraced into a single perspective that values acquiring key knowledge quickly in order to not miss out on an important opportunity. The same can be said of the day we are born being the day we begin to die. While viewing birth and death as distinct events is common in the West, there are many Aboriginal groups and people from other cultures for whom this division simply does not exist (i.e., they have embraced the paradox). Being able to embrace paradox is a key ingredient to both improvisational theater and organizational strategy. That is, just as there is opportunity in an improvised death on stage to allow for an entirely new scene to be born, so too must strategists be willing to plan, yet also be willing to throw away the plan (figuratively or literally) as dynamic environments unfold.

The parallels between strategy formulation and improvisation are many and include the notion that organizations need to plan, yet be nimble enough to deviate from the plan. Kanter in her article entitled, "Strategy as improvisational theatre," suggested that companies that want to innovate have to be willing to throw out "the script" (aspects of planned strategy) in order to "improvise their way to new strategies" (i.e., emergent strategy).[99] While throwing out the script might be extreme, in that it would insinuate following a totally emergent approach, being willing to throw out the parts of the script that are not working optimally allows the strategy to evolve in a planned emergence fashion. This can also be a suggested approach for companies to foster innovation.[100]

The Future of Strategy Creation and Implementation

To be successful in the long term, the methodology employed by an organization to create and implement strategy must recognize the inherent need for both the planned and emergent aspects of this complex process. Recognition must be afforded to the

[97] Mintzberg and Waters (1985).

[98] Canadian Oxford Dictionary (2004).

[99] Kanter (2002).

[100] Kanter (2002).

concept that strategy is both art and science[101] and that a strategy's evolution cannot be controlled but only guided due to the complex and chaotic nature of the internal and external environments in which an organization must operate.

Contrary to current thought in many operating organizations and educational institutions, strategy creation does not end with the dissemination of a strategic plan. Due to the evolving nature of a strategy as it interacts with an organization's environment, the strategy that is eventually implemented has continued to transform throughout its implementation period. The question that decision makers in any organization must address is whether or not they will play a guiding role in their strategy's transformation because with or without their input, the strategy will evolve.

To achieve a guiding role in a strategy's transformation, a management team must set aside time to focus on strategy issues, not just as part of an annual strategic planning ritual but as an ongoing part of the management function. This is often easier to conceptualize than to accomplish because there are always pressing operational issues to be attended to such as monthly and quarterly financial metrics, manufacturing problems, significant personnel issues, and others. Even when a management team has the best intentions to focus on strategy, it is difficult to accomplish in the day-to-day grind of running an organization and satisfying stakeholders who are often focused on short-term goals.

For an organization to successfully guide its strategy's evolution as it interacts with the environment, environmental factors that might affect the strategy must be monitored on an ongoing basis. Further, time must be formally allocated to focus on strategy and to allow discussion within the decision-making group in view of environmental monitoring and required actions or adjustments to the strategy. Further, other factors such as incentive structure must be aligned with strategy. For example, if decision makers are effectively told to focus on short-term objectives through incentive plans that are triggered solely by the accomplishment of short-term objectives, it should not be surprising that they are not focused on strategy.

If the future of strategy creation and implementation is to be more successful than the past, educators and managers must acknowledge the importance of both the planned and emergent aspects of strategy. These two strategy concepts have important roles to play and feed off each other as a strategy transforms during implementation. To be successful, managers must focus on strategy throughout the year and guide their strategies so they remain viable in the face of changing internal and external environments.

References

Andersen TJ (2004) Integrating decentralized strategy making and strategic planning processes in dynamic environments. J Manag Stud 41:1271–1299

Andrews KR (1971) The concept of corporate strategy. Dow Jones-Irwin, Homewood

[101] Parnell and Lester (2003).

Ansoff HI (1991) Critique of Henry Mintzberg's 'The design school: reconsidering the basic premises of strategic management'. Strateg Manag J 12(6):449–461
Ashill NJ, Frederikson M, Davies J (2003) Strategic marketing planning: a grounded investigation. Eur J Market 37(3/4):430–460
Bain and Co. (2003) Bain study reveals how firms are using three main analytical tools. Financial Times, 4th Sept 2003
Blythe J, Zimmerman A (2004) Strategic planning for global markets. Market Rev 4:369–384
Boyd BK (1991) Strategic planning and financial performance: a meta-analytic review. J Manag Stud 28(4):353–374
Boyd BK, Reuning-Elliot E (1998) A measurement model of strategic planning. Strateg Manag J 19:181
Bradbury H, Lichtenstein BMB (2000) Relationality in organizational research: exploring the space between. Organ Sci 11(5):551
Brews PJ, Hunt MR (1999) Learning to plan and planning to learn: resolving the planning school/learning school debate. Strateg Manag J 20(10):889–913
Canadian Oxford Dictionary (2004) In: Katherine Barber (ed.). 2nd edn. Oxford University Press: Toronto, ON
Crossan MM (1998) Improvisation in action. Organ Sci 9:593–599
Crossan MM, Sorrenti M (1997) Making sense of improvisation. In: Walsh J, Huff J (eds) Advances in strategic management, vol 14. pp 155–180. Greenwich, CT: JAI Press
Depperu D, Gnan L (2006) The role of the competitive context in the business strategy-formation process. Int Stud Manag Organ 36:110–130
Entrekin L, Court M (2001) Human resource management practice: adaptation and change in an age of globalization. International Labour Office, Geneva, p 14
Falshaw JR, Glaister KW, Tatoglu E (2006) Evidence on formal strategic planning and company performance. Manag Decis 44(1):9–30
Ginter PM, Rucks A, Duncan WJ (1985) Planners' perceptions of the strategic management process. J Manag Stud 22(6):581
Grant RM (1995) Contemporary strategy analysis: concepts, techniques, applications, 2nd edn. Blackwell, Cambridge
Grant RM (2003) Strategic planning in a turbulent environment: evidence from the oil majors. Strateg Manag J 24:512
Greenley GE (1994) Strategic planning and company performance: an appraisal of the empirical evidence. Scand J Manag 10(4):383–396
Grove AS (1997) Navigating strategic inflection points. Bus Strategy Rev 8(3):11–18
Harrington RJ et al (2004) A question of fit: the links among environment, strategy formation, and performance. J Bus Manag 10:15–38
Holloway DA (2004) Strategic planning and informed discourse: reality or rhetoric. Crit Perspect Account 15(4–5):469–483
Hopkins WE, Hopkins SA (1997) Strategic planning-financial performance relationships in banks: a causal examination. Strateg Manag J 18(8):635–652
Kanter RM (2002) Strategy as improvisational theater. MIT Sloan Management Review 76–81
Kjaergaard AL (2009) Organizational identity and strategy. Int Stud Manag Organ 39(1):50–69
Lee TW, Mitchell TR, Sablynski CJ (1999) Qualitative research in organizational and vocational psychology, 1979–1999. J Vocat Behav 55:161–187
Levy D (1994) Chaos theory and strategy: theory, application, and managerial implications. Strateg Manag J 15:167–178
Miller CC, Cardinal LB (1994) Strategic planning and firm performance: a synthesis of more than two decades of research. Acad Manag J 37(6):1649
Miller D, Friesen PH, Mintzberg H (1984) Organizations: a quantum view. Englewood Cliffs, Prentice-Hall
Miller D, Droge C, Toulouse J-M (1998) Strategic process and content as mediators between organizational context and structure. Acad Manag J 31(3):544–569

Mintzberg H (1977) Strategy formation as a historical process. Int Stud Manag Organ 7:28–40
Mintzberg H (1987) Crafting strategy. Harvard Business Review 65:73
Mintzberg H (1990) The design school: reconsidering the basic premises of strategic management. Strateg Manag J 11:171–195
Mintzberg H, Lampel J (1999) Reflecting on the strategy process. MIT Sloan Management Review 40:21–30
Mintzberg H, Waters JA (1985) Of strategies, deliberate and emergent. Strateg Manag J 6:257–272
Moorman C, Miner AS (1998) Organizational improvisation and organizational memory. Acad Manag Rev 23:698–723
Parnell JA, Lester DL (2003) Towards a philosophy of strategy: reassessing five critical dilemmas in strategy formation and change. Strateg Change 12:291–303
Porter ME (1996) What is strategy? Harvard Business Review:61–78
S&T Encyclopedia (2007) McGraw-hill encyclopedia of science and technology online, 2007. http://connect.carleton.ca/cp/tag.f394e61f9e7ba7f8.render.userLayoutRootNode.uP?uP_root=root&uP_sparam=activeTab&activeTab=u11l1s154&uP_tparam=frm&frm=frame
Schäffer U, Willauer B (2003) Strategic planning as a learning process. Schmalenbach Business Review (SBR) 55:86–107
Sminia H (2009) Process research in strategy formation: theory, methodology and relevance. Int J Manag Rev 11(1):97–125
Thune SS, House RJ (1970) Where long-range planning pays off. Bus Horiz 13(4):81
Wiltbank R et al (2006) What to do next? The case for non-predictive strategy. Strateg Manag J 27(10):981–998