Chapter 19

Supply Chain Preparedness

Supply chain security has long been a problem for practitioners. As you will see in this chapter, this is not a new problem. The events of September 11, 2001and the events of the rest of that week, emphasized the importance of security and the potential impacts of interruptions to the supply chain. This is not a United States-only problem—Supply Chain Security is an international problem with large implications for everyone involved in supply chain management and operations management. But the time has come to look at other impacts to supply chains that may disrupt the continuous flow of goods and services to the customers.

Why should you care about supply chain security? As long as the items that you order arrive, are you really concerned with how they get there and whether or not the items are secure while in transit? This goes back to "supply chain done well is all but invisible." Supply chain risks come in the form of panic buying during the pandemic, supplier failures, natural disasters as we saw at the Port of New Orleans during and after Katrina in 2005 or the problems at Port-Au-Prince after the earthquake in 2010, Puerto Rico impacts from the 2018 hurricanes, terrorist attacks, employee theft, or risks from regulatory requirements. The 2016 earthquakes in Japan impacted supply chains as far away as Kansas City, KS.

What is supply chain security and if it is so important how come it is not discussed in most operations management textbooks? The goal of this chapter is to not only familiarize the student of operations management with the topic of supply chain security but to also demonstrate to the student the importance of end-to-end supply chain security throughout the entire supply chain and the costs associated with supply chain security. At the same time, the goal is to show the importance of supply chain preparedness in operations management and in business in general.

There is not much more in the form of strategy for supply chain security today than there was in the Wu Province of China in 512 B.C. Sun Tzu lived in the Wu Province and wrote in the

first chapter of his book *The Art of War* that protecting supply lines was important. In fact, he went so far as to say that to be successful in any operation, you must protect your supply lines. The United States published a *National Strategy for Homeland Security* in 2007 that mentions no more about supply chain security than Sun Tzu's work 2500 years earlier. The National Supply Chain Security Strategy from 2012 (see Figure 19.1) has a longer executive summary than the strategy document itself. A lot of energy is going into writing about supply chain security but not a lot of energy is going into actually preparing for interruptions in the supply chain.

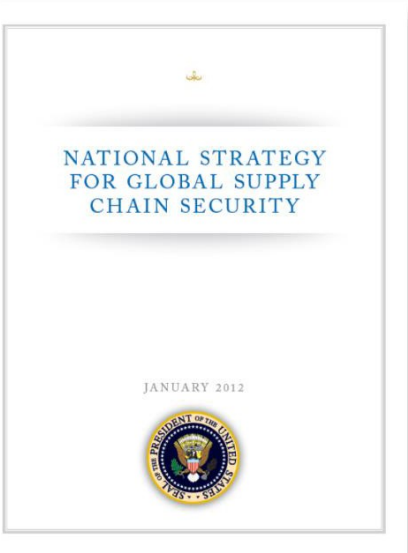


Figure 19.1: National Strategy for Global Supply Chain Security Cover

Supply chain security is all the actions taken to ensure the security of items passing through the supply chain. Supply chain security has major impacts on the actions of key players throughout the supply chain and can impact customer responsiveness and supply chain costs. According to several accounts, the impact of an attack on a major port within the United States could cost as much as $20 billion daily to the US economy. According to *FORTUNE* magazine, the costs to the US economy as a result of the terrorist attacks of September 11, 2001, is approximately $50–80 billion a year as a result of increased inventory levels, increased security measures, and higher transportation costs.

Counterfeit products are the latest threat to supply chains. Amazon announced in their 2018 that they had a major issue with counterfeit products. This was followed by a claim from Apple that as much as 90% of the Apple products sold through Amazon were fake. In 2020, the growth of e-commerce as a direct reaction to coronavirus fears led to a growth in fraudulent products being offered to consumers.

The fact that supply chains continue to lengthen and become more globalized contributes to the complexity and security implications of supply chains. Although the terrorist activities around the world have put the focus of supply chain security on attacks to the supply chain from terrorists, the fact is that the risks to supply chains requiring attention and impacting security are greater than just terrorist attacks as we will see in this discussion of supply chain security. The threats to supply chains can come internally or externally to the supply chain.

Is supply chain security really a problem? Here (Figure 19.2) are some of the threats to twenty-first century Supply Chains:

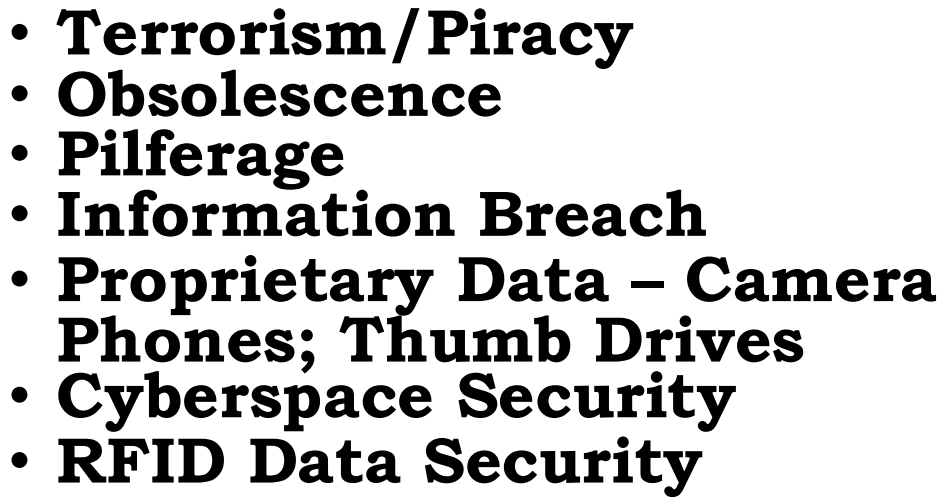


Figure 59.2: Threats to Supply Chains

Let's take a look at each of these threats to supply chains. The most commonly associated threat to supply chains is terrorism. Another form of terrorism that has received more than cursory attention lately is the threat of piracy. Terrorism threats receive more attention than other potential threats to supply chains.

Obsolescence of materials and products is a threat to supply chains as was discussed in previous chapters. Although this threat to supply chain operations and operations management success is critical, it is not a threat in the sense of supply chain security. But proper planning and careful inventory management can prevent this from being an issue.

Pilferage and theft within supply chains is a growing problem. This comes in the form of employee pilferage and theft along the entire supply chain. Theft by employees in distribution centers in the United States alone is reported as high as $60 billion annually (two studies were

released in 2019 that placed this issue at between $10 and $60 billion depending on which study you believe). According to one investigator specializing in distribution center theft this figure may be only 10 percent of the actual losses since some companies do not want to report employee theft.

As we will see in the next section when we look at some recent headlines about security, information breaches are becoming a larger and larger problem as more business is completed on the Internet. A recent article in the *Kansas City Star* newspaper looked at the proliferation of information on the Internet as a result of e-commerce and social networking sites. Everyone read about the 2013 security breach at Target and the trickle-down effects from that debacle—this all started with a supplier's computer system and allowed a backdoor into Target's system.

Tied to information breaches and loss of data is the theft of proprietary information by disgruntled employees. Several years ago, a secretary at Coke was arrested by Federal Agents for trying to sell the proprietary formula for Coca Cola to Pepsi. Twenty-five years ago, a good computer had a 100 MB hard drive (yes, you read that right, 100MB – about the size of this textbook with pictures). Today you can buy a 256 GB thumb drive that can hold thousands of pages of proprietary data and information if a disgruntled employee wanted to steal information and sell it to competitors. Cell phones with cameras used to be a science fiction story; today any employee can capture data from work on the phone and pass it to others easily or with a camera pen for that matter. Some companies do not allow cell phones on tours of the factory—the reason given is to prevent distractions; however, when questioned privately several admit that the ability to take pictures of proprietary operations with the phones is the reason for the rules. The 3M plant in Panama makes sanding disks and buffing pads using robotics, they do not allow cameras as they don't want their competition to see what they are doing.

RFID security is a grave concern as discussed earlier. If you can read your tag's information, who else can read the information thus making your data available to many and allowing potential thieves to target shipments? It was not until 2013 that developers started working on an encrypted RFID tag. This after over 20 years of commercial use for RFID tags. This is from a 2016 article on encrypted RFID tags:

"Radio frequency identification (RFID) chips have made cashless payments commonplace and opened the way to automatic inventory control. However, they've also made it possible for credit card details and other private information to be stolen wirelessly. To make

things a bit more secure, MIT and Texas Instruments are developing an "unhackable" RFID chip that's designed to fend off information-stealing attacks."[121]

There are other potential problem areas for supply chains that need to be discussed before we move on. As much as 66% of all sealift containers coming into the United States arrive through 20 major ports. Although this sounds significant from a security perspective, it becomes even more significant when drilling down a bit and realizing that more than 58% of the inbound containers to the United States come in through the Ports of New York/New Jersey, Los Angeles, and Long Beach. And this becomes even more significant from a supply chain security perspective when one realizes that approximately 44% of the inbound cargo containers arriving in the United States come to the West Coast Ports of Los Angeles and Long Beach. From a security perspective, these threats or potential problem areas are a result of the lengthening of supply chains as a result of globalization of supply chains and the continued trend to off-shore manufacturing operations to emerging countries. Perhaps the lessons being learned during the 2020 pandemic will result in more operations being near-shored (Mexico, Latin America) or even brought back to the US which would shorten supply chains and possibly reduce some risks associated with longer supply chains.

A Sampling of Supply Chain Security Related Headlines:

- Kids hospitalized after eating counterfeit Nerds laced with THC
- Natural Disasters – follow up report on Puerto Rico
- Floods
- Factory Fires
- Cyber attacks –
- Panic Buying
- Citrus Australia trials blockchain traceability system
- Coronavirus increases online shopping, but buyers fear fakes

As more companies start to experience supply chain interruptions, headlines such as the ones listed above continue to increase. As more companies discover the risks to their supply chains, more executives are becoming interested in preventing, mitigating, or eliminating supply

[121] https://newatlas.com/unhackable-rfid-team-credit-cards/41707/, accessed 20 April 2020.

chain risks. Even though the focus remains on terrorist threats, supply chain security includes supply chain preparedness which also includes the risks from natural disasters as has been seen from Hurricane Katrina in 2005 and the impacts to the shipping into and out of New Orleans; the impacts to the food supply chain as a result of the British Petroleum oil catastrophe in the Gulf of Mexico; the impacts from the earthquakes in Japan in 2012 and 2016; the impacts to the medical supply chain after the hurricanes ravaged Puerto Rico in 2018; and the impacts in shipping from Hurricane Harvey's deluge in Houston in 2018.

"We have proved to our management that good security is good business."

—Ann Lister of Texas Instruments

Examples of supply chain security problems, not making headlines:

- Distribution Center, 2014: "A big problem that we are facing now is the printing of shipping labels at home and employees picking shipments for themselves and putting on official looking shipping labels."
- Major Distributor, Dec 2006: A company I was working with during this time had a security problem. This particular company used RFID tags and an Automated Manifesting System to track and process electronics shipments. As a result of this technology and partnerships with certified suppliers, this particular company was in the habit of accepting shipments based on the RFID tags and the Automated Manifesting System.

  This particular truck arrived at the dock of the Third Party Logistics Provider (3PL) providing distribution center management for the company. This truck backed up to the dock at the distribution center to the dock door designated at the entry gate. The driver dropped the trailer at the dock door and left. Thirty minutes later another tractor hooked up to the trailer and departed the yard. No one at the security gate suspected anything as the average time to offload a truck was about 30 minutes.

  Six months later the company, their insurance company, the trucking company, and their insurance company were still in discussions on who was liable for the disappearance of over $3 million (USD) in electronics.
- Locks on trucks: Apparently thieves in the New York area have discovered that getting access to cargo in the back of a semi-trailer is not that difficult. All that is needed is a Bic lighter. Holding the lighter under the large locks on the back of the trailer for a set period

of time allows the thieves to then hit the lock with a hammer and the lock will split wide open giving access to the thieves to all that is in the trailer. This is why you will see trailers parked back to back in trailer yards when not on the road.

- SAFE Port Act: The full title of this law is the SECURITY AND ACCOUNTABILITY FOR EVERY PORT ACT OF 2006. The act was signed into law on October 13, 2006. This law defines the supply chain as: *"INTERNATIONAL SUPPLY CHAIN. —The term ''international supply chain'' means the end-to-end process for shipping goods to or from the United States beginning at the point of origin (including manufacturer, supplier, or vendor) through a point of distribution to the destination."*[122]

  This law provided for unannounced inspections of cargo containers and added more legitimacy to the Customs-Trade Partnership Against Terrorism (C-T PAT). The law also set forth for the scanning of containers at ports of entry. "*SCANNING CONTAINERS.—Subject to section 1318 of title19, United States Code, not later than December 31, 2007, all containers entering the United States through the 22 ports through which the greatest volume of containers enter the United States by vessel shall be scanned for radiation. To the extent practicable, the Secretary shall deploy next generation radiation detection technology."*[123]

The law also established the requirement for a strategy for improving the "International Supply Chain." Part of this strategy resulted in 2010 of what has become known as the 10+2 Reporting Requirements. According to the Customs and Border Patrol, "The Security Filing, commonly known as the '10+2' initiative, is a Customs and Border Protection (CBP) regulation that requires importers and vessel operating carriers to provide additional advance trade data to CBP pursuant to Section 203 of the SAFE Port Act of 2006 and section 343(a) of the Trade Act of 2002, as amended by the Maritime Transportation Security Act of 2002, for non-bulk cargo shipments arriving into the United States by vessel." These reporting requirements must be done electronically via an Automated Manifesting System or an Automated Broker Interface. This

[122] The SAFE Port Act is Public Law 109-347.

[123] PUBLIC LAW 109–347—OCT. 13, 2006, **Subtitle C—Port Operations SEC. 121. DOMESTIC RADIATION DETECTION AND IMAGING.**

reporting is commonly called the 10+2 Reporting Requirements. Figure 19.3 shows the "10" reporting items for shippers/importers:

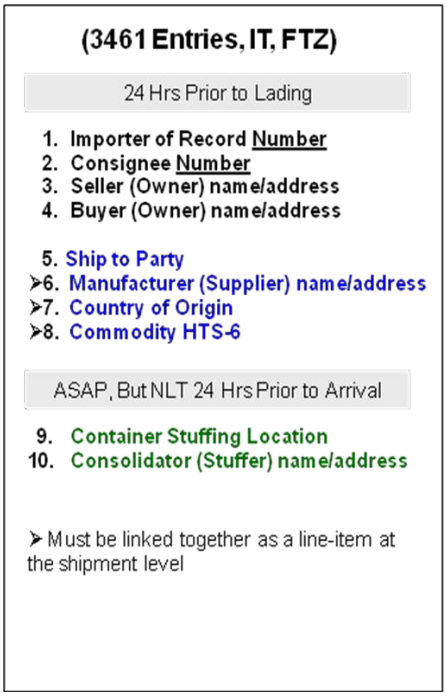


Figure 19.3: Reporting Requirements[124]

In addition to the "10" reporting requirements for shippers, the carriers are required to report their vessel stow plan and any container status messages.

- Scanning of Containers: The goal of the scanning of all containers coming into the United States is to identify any potential dirty bomb coming into the United States in any one of the approximately 12 million containers coming into the country. The use of X-ray machines and radiation detectors is the plan for this scanning. The concern of the workers at ports is the effect to the workers from the exposure to large X-ray machines. Included in this effort are the Container Security Initiative, the Megaports Initiative, and the

[124] http://www.cbp.gov/xp/cgov/trade/cargo_security/carriers/security_filing/, accessed May 30, 2010.

Secure Freight Initiative. The National Strategy for Homeland Security explains the process as[125]:

*"The **Container Security Initiative** (CSI) creates a security regime to prescreen and evaluate maritime containers—before they are shipped from foreign ports—through automated targeting tools, ensuring that high-risk cargo is examined or scanned. The **Megaports Initiative** is a Department of Energy program in which the United States collaborates with foreign trade partners to enhance their ability to scan cargo for nuclear and other radiological materials at major international seaports.*

*The **Secure Freight Initiative** is a comprehensive model for securing the global supply chain that seeks to enhance security while keeping legitimate trade flowing. It leverages shipper information, host country government partnerships, and trade partnerships to scan cargo containers bound for the United States."*

The Department of Homeland Security (DHS) initiated the first phase of the Secure Freight Initiative in 2007. This phase included the use of "existing technology and proven nuclear detection devices" at six major ports of embarkation shipping to the United States. According to the DHS, "Containers from the ports will be scanned for radiation and information risk factors before being allowed to depart for the United States." The first six ports in this program are: Port Qasim (Pakistan), Port Cortes (Honduras), Southampton (United Kingdom), Port Salalah (Oman), the Port of Singapore, and Port Busan (South Korea).

There is a link between homeland security for the United States and any country and supply chain security as discussed in ***The National Strategy for Homeland Security***. This document was published in October 2007. The strategy starts with:

"America is at war with terrorist enemies who are intent on attacking our Homeland and destroying our way of life…… The purpose of our strategy is to guide, organize, and unify our Nation's homeland security efforts. It provides a common framework by which our entire Nation should focus its efforts….

---

[125] For more on the National Strategy for Homeland Security go to http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf

The private and non-profit sectors also must be full partners in homeland security. As the country's principle providers of goods and services, and the owners or operators of approximately 85% of the Nation's critical infrastructure, businesses have both an interest in and a responsibility for ensuring their own security. The private sector plays key roles in areas as diverse as supply chain security….

Our vast land and maritime borders make it difficult to completely deny terrorists and their weapons access to the Homeland."[126]

- Containers in Pakistan: During Operation Enduring Freedom, all cargo that could not be brought in by air arrived via ground shipment through Pakistan. The thieves in Pakistan figured out that the military containers were weighed when they leave the port of entry and are then weighed again upon entry into Afghanistan. The solution of the thieves was to cut the back of the container off, empty the supplies and materials in the container, and fill it back with filled sand bags until the proper weight was achieved and then weld the back onto the container. This left the security seals intact and gave the illusion of a container that had not been tampered with as it crosses the border.
- C-T PAT: This started after September 11, 2001 as a voluntary partnership between the Customs and Border Patrol and Commercial companies. By the time the SAFE Port Act, became law, this voluntary organization had over 9000 participants. The participating companies go through an audit and certification process to demonstrate that they have control of their containers and products from the time the products are loaded into the containers. This then provides the participants a "fast-pass" through the inspection processes established by the SAFE Port Act. "Partners in protection" is the Canadian equivalent of C-T PAT.

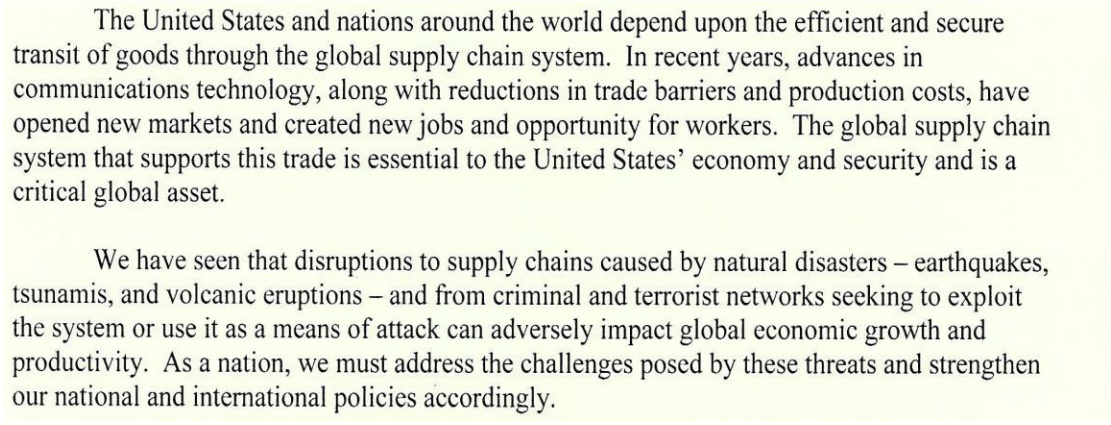
- ISO Standards for Supply Chain Security: According to the International Standards Organization, "The **ISO 28000 series of standards** on supply chain security management systems, which have just been upgraded from their status of Publicly Available Specifications to that of fully fledged International Standards, will help to reduce risks to people and cargo within the supply chain. The standards address

---

[126] National Strategy for Homeland Security, Homeland Security Council, October 2007, pp. 1–6.

potential security issues at all stages of the supply process, thus targeting threats such as terrorism, fraud and piracy."

- Terrorism Risk Insurance: The US Terrorism Risk Insurance Act was signed into law by former President George W. Bush in 2002 and renewed in 2007 with an expiration date of 2018. The goal of this law is to supplement commercial insurance companies in the event of terrorist attacks such as 9/11. On December 20, 2019, the President signed into law the Terrorism Risk Insurance Program Reauthorization Act of 2019 (Pub. L. 116-94, 133 Stat. 2534) [2019 Reauthorization Act], which extended TRIP through December 31, 2027.
- The National Strategy for Global Supply Chain Security was published in 2012.[127] The opening paragraphs for the strategy are shown in Figure 19.4.



The United States and nations around the world depend upon the efficient and secure transit of goods through the global supply chain system. In recent years, advances in communications technology, along with reductions in trade barriers and production costs, have opened new markets and created new jobs and opportunity for workers. The global supply chain system that supports this trade is essential to the United States' economy and security and is a critical global asset.

We have seen that disruptions to supply chains caused by natural disasters – earthquakes, tsunamis, and volcanic eruptions – and from criminal and terrorist networks seeking to exploit the system or use it as a means of attack can adversely impact global economic growth and productivity. As a nation, we must address the challenges posed by these threats and strengthen our national and international policies accordingly.

Figure 19.4: Supply Chain Security Strategy (Government, 2012)

Risk Analysis and Supply Chain Security

"If you do things the way you've always done them, you'll get the same things you've always got."

—Darrell Waltrip (Three-time NASCAR Winston Cup Champion)

---

[127] Go to:

http://www.whitehouse.gov/sites/default/files/national_strategy_for_global_supply_chain_security.pdf for more information on this strategy.

The goal of supply chain risk analysis is twofold. The first goal is to ensure that you do not do things the way they have always been done in the past. The second goal of risk analysis is to identify the risks to the supply chain and the severity of the impacts if the risks become reality. Supply Chains are inherently complex, dynamic, and fluid, characterized by uncertainty, ambiguity, and friction. These characteristics cloud the operating environment. These supply chain characteristics also create risks to the supply chain. The best way to identify risks to your supply chain is to walk the process to completely understand the potential risks to the supply chain.

Once the risks have been identified the next step is to implement a risk management program. The goal of the risk management program is to implement processes that will eliminate, minimize, or mitigate the occurrence and/or impact of any potential risk. The goal is to prevent any catastrophic risk to the supply chain. Just what is a catastrophic risk? Anything that can slow or stop the flow of supplies through the supply chain is potentially a catastrophic risk. It could be a recalled product as Mattel learned in 2008, it could be the inability to meet shipments as Hershey learned in 1999, or as Toys-R-Us learned in the same year. The goal of a good risk management program is to ensure that the problems do not become catastrophic by hitting the front page of *USA Today* or the headlines of CNN.

Historical perspective of Supply Chain Security

Risks to supply chains are not a twenty-first century invention. This has been a problem for at least 2500 years. In *The Art of War,* Sun Tzu wrote that the key to success in any operation depended on protecting and securing supply lines. The Japanese Imperial Navy clearly understood supply chain security as they moved across the northern Pacific Ocean enroute to Pearl Harbor.

In his book, *Vietnam Logistics,* General Joseph Heiser wrote, “There were no secure rear areas.” He went on to explain that the fuel lost from the pipelines from theft was almost as great as the amount of fuel delivered to the intended recipients.

The pirates of the Caribbean were real and made their fame by interdicting supply lines to the “New World” long before they became part of a ride at Disney World and later a series of movies. Blackbeard based his crew out of the Ocracoke, North Carolina and made his fortune doing the same off the East Coast of the United States. The goal of the pirates in the 1700s was

to stop shipments moving from the Old World to the New World and take what they wanted from the ships heading west.

In the United States, the Native Americans realized very early that the best way to slow the expansion of the settlers moving west was to attack the wagon trains. Their goal was to stop the supply and resupply of the settlers. The reaction to counter these attacks was the establishment of outposts or military forts throughout the western United States to protect the supply lines.

The German Navy understood the same concept during World War II and did their best to slow the resupply of Allied Forces by attacking the ships at sea in the Atlantic Ocean and as close as just off the coast of North Carolina. They understood that if the supply lines were severed, the ability to sustain combat operations was severely diminished. The Germans even contemplated destroying the Panama Canal to interrupt the flow of supplies.

During the American Civil War, the goal to interdict the supply chains led to the actions that produced the first Congressional Medal of Honor recipients. It also led to a Disney movie, *The Great Locomotive Chase*, in 1956. Understanding that interdicting the supply lines from Atlanta to Chattanooga would cut off resupply of the Confederate States of America soldiers, the Union soldiers infiltrated and attempted to steal a locomotive with the intent of destroying all of the bridges north of Atlanta. Likewise, the goal of the Siege of Petersburg, Virginia was to sever the rail lines heading north from North Carolina to Richmond. Severing the rail lines would cut off the resupply of the soldiers of General Robert E. Lee's Army. General Sherman attempted to stop the rebuilding of the rail in Georgia during his march to the sea. To prevent reuse of the rail, General Sherman had the rail removed, heated and wrapped around trees as shown in Figure 19.5.

Figure 19.5 Rail Wrapped Around a Tree as Seen in The American Civil War Museum

Protecting supply chain operations has been a problem and an issue for most of recorded history. It is just as important today as it has been over time. The difference today is that supply chains are inherently more complex and globalized, thus presenting more potential opportunities to interrupt or interdict and impede supply chain operations. The old Oldsmobile commercial stated, "This is not your Dad's Oldsmobile." Today's supply chain is "Not your Dad's Supply Chain!" The potential risks are greater from inside and outside the supply chain.

Food/Pharmaceutical Supply Chain Security

One of the areas that has received a lot of attention since the 9/11 attacks is the food supply chain and the pharmaceutical supply chain. The concern about the food supply chain led to the requirement for Country of Origin reporting requirements. These reporting requirements were designed to prevent bio-terrorism activities and are now part of the "10+2" reporting requirements discussed earlier.

However, let's take a look at some of the most recent "bio-terrorism" incidents in the United States. Most of these are not bio-terrorism at all but still had great impacts on supply chains and fall under the umbrella of supply chain security.

- Peter Pan Peanut Butter: In 2007, every jar of Peter Pan Peanut Butter was recalled due to E-coli contamination.
- Just one year earlier, in 2006, all of the fresh Spinach was recalled because of E-coli. Like the Peter Pan situation, the E-coli was not bio-terrorism but the impact on the supply chain—both forward and reverse was dramatic.
- E-coli was also responsible for problems experienced by Chi-Chi's in 2003 and Taco Bell in 2005.
- In 2008 there were salmonella and E-coli scares in the fresh foods industry. First all of the fresh lettuce was taken off the shelves; then when that did not fix the problem, all of the peppers were taken off the shelves. Turns out there were problems with the supply chain but not in the bio-terrorism area, only in the handling and processing of the foods—all within the United States.
- The largest incident of salmonella poisoning in recent history was another example of supply chain impacts—especially going backward. This like the other examples was not an incident of supply chain bio-terrorism. It was simply a problem of poor control and handling in the supply chain—primarily in the "Make" function of the supply chain.

  In this particular incident the Peanut Corporation of America provided products that were contaminated with salmonella. This resulted in over 3921 separate SKUs being recalled and almost 40,000 reported cases of salmonella poisoning. Prior to the use of Peanut Corporation of America (PCA) products, Kellogg hired a consultant company to analyze the operations at PCA. Kellogg used the lowest bidder process for this consultant and was told that there were no problems at the PCA plant. Nestle used a different consultant. This consultant reported potential cross contamination of products, rat feces in the plant, roaches in the plant and recommended against the use of the company's products. Kellogg, the parent of Keebler, had multiple products recalled due to contamination while Nestle had no products recalled due to salmonella contamination from the PCA products.
- 2014; Listeria found in cantaloupes from Colorado. In this incident a number of people died from the listeria poisoning.

- 2018 and again in 2019: Recall of Romaine lettuce due to e-coli contamination.

While bio-terrorism is definitely a potential international supply chain security problem, the most recent incidents reported have not been terrorism but self-inflicted problems. The security of the pharmaceutical supply chain poses a grave concern for everyone. In the introduction, we mentioned counterfeit items as a risk to supply chains. In the pharmaceutical supply chain this poses a greater risk. One of the counters to this risk is the use of RFID tags to identify products, lot numbers, and expiration dates.

As was seen in the recent Tylenol recall (2010), the use of ingredients that are not pure or controlled can cause problems in the pharmaceutical industry. Because of the potential impacts of contamination of ingredients in pharmaceutical products, supply chain security becomes a larger issue with potentially wider consequences. As more products are sourced globally, this concern increases. According to the Pharmaceutical Security Institute (http://www.psi-inc.org):

"Counterfeit medicinal products are a threat to the health and safety of patients around the world. They range from drugs with no active ingredients to those with dangerous impurities. They can be copies of branded drugs, generic drugs or over-the-counter drugs."[128]

The link to the supply chain is explained by the Pharmaceutical Security Institute (PSI):

"Pharmaceutical theft is defined as an illegal taking of medicines. Thefts include burglary, robbery, or an embezzlement of goods. The responsible individuals may be insiders such as employees, or outsiders such as professional thieves. The theft may occur anywhere in the distribution chain such as at the site of manufacture, freight forwarder, distribution centers, warehouses, pharmacies, or hospitals."[129]

Another aspect of pharmaceutical supply chain security being countered by the use of RFID tags is deemed "Illegal Diversion" by the PSI. Illegal Diversion is defined and described as: *"Illegal diversion occurs when a genuine pharmaceutical product is approved and intended for sale in one country, but is then illegally intercepted and sold in another country. These*

---

[128] http://www.psi-inc.org/index.cfm, accessed May 31, 2010.

[129] http://www.psi-inc.org/counterfeitSituation.cfm, accessed May 31, 2010.

schemes are often accomplished through the use of false statements or declarations."[130] The Associate Commissioner for Policy and Planning for the US Food and Drug Administration in testimony before Congress stated: "While the United States drug supply is among the safest in the world, we believe there are increasingly sophisticated threats from drug counterfeiters. Organizations and individuals who peddle fake medicines put unsuspecting patients at risk, by exposing them to unknown contaminants and denying them medicines known to be safe and effective at treating their medical ailments. Counterfeit drug products and illicit drug diversion are major concerns to FDA."[131]

The global impact of counterfeit and diverted products within the pharmaceutical supply chain continues to grow as supply chains become more globalized. Pfizer has taken a plan of attack of buying these counterfeit products and analyzing them to see what components are being used. One of their latest discoveries from counterfeit batch was that there were only 4% active ingredients and 96% concrete dust.

Other counterfeit items impacting the supply chain include counterfeit condoms, counterfeit cigarettes, and counterfeit liquors and wines. In fact, in 2012 there were more bottles of 1992 Rothschild wine in China than were actually bottled originally. In 2012 there was a court case involving fake 200-year-old wine and later an article online giving the details of how to counterfeit antique wines. The impact of these products in supply chain security and supply chain confidence is great and has ripple effects through the entire supply chain.

A Global Perspective

As the pandemic of 2020 demonstrated to everyone, supply chains are global, and a global pandemic can play havoc with the supply chain. The interrelationship of countries through the supply chain require global supply chain security and preparedness.

---

[130] Ibid.

[131] http://www.fda.gov/NewsEvents/Testimony/ucm111840.htm, accessed May 29, 2010.

The Port of Rotterdam

Rotterdam is the largest port in Europe with over nine million twenty foot equivalent containers coming into the port each year. This means over 25,000 containers every day of the year coming into Rotterdam. This drives the over 900 barge moves daily to approximately 72 locations reachable by barge and over 200 rail moves each day from the port to customer locations to the east. The rail and barge movements into and out of Rotterdam provide support to the over 220 million people that live within a 600 mile radius of Rotterdam.

In addition to containers, rail movements, and barge moves, The Netherlands is home to over 9000 distribution centers with over $64 billion (USD) in logistics operations. These operations help to feed the logistics operations in Belgium where over 13% of the shipments move through the country via rail and into Germany where approximately 15% of the shipments arrive via rail.

Rail security in Europe, like in the United States is critical for success of supply chain operations. In the United States, there are only four major rail bridges across the Mississippi River. Every rail bridge in the United States and in Europe present targets of opportunity for supply chain security lapses.

Preparedness

It is time to move from a narrow-minded focus on supply chain security as anything that is manmade to interrupt the supply chain. This focus has helped to reduce the number of terrorist attacks globally but as we have pointed out earlier, natural events can impact the supply chain just as severely and occur more frequently.

Companies and countries need to start contingency planning based on impacts from natural events such as hurricanes, tornados, earthquakes, tsunamis, volcanos, and other major weather related incidents. This contingency planning is called **preparedness**. Every company needs to take a close look at their supply chain and start making plans to ensure that their customers are ensured an uninterrupted flow of products regardless of what happens.

According to Motorola University, the first step of six sigma is to define who the customer is, what the customer wants and how "we can do it better than the competition." This is the foundation of preparedness – what do we need to do to take care of the customer?

Summary

Supply chain security is not a new issue but one that has the potential to have an enormous impact on the success and profitability of a company's supply chain operations. Sun Tzu warned us 2500 years ago to protect our supply lines to be successful in any operation. The supply chains of Sun Tzu's day were much less complicated than the supply chains of the twenty-first century. Supply chains were mostly local in Sun Tzu's day; supply chains are mostly globalized and inherently complex in today's world.

Supply chain security starts with a process walk of the supply chain to identify potential risks and then putting a risk management plan in place to eliminate the risks if possible. If elimination of the risk is not possible, the risk management program should seek to minimize or mitigate the impact of the potential occurrence of the risk. The goal is to protect the items in the supply chain from end to end and ensure that the products reach the intended customer without delay.

There is a link between supply chain security and homeland security—this is not a US-unique problem. There is also a link between supply chain security and velocity in a supply chain. The more secure a supply chain is the greater the chance that it may move a little slower. However, it is much better to move a little slower than stop moving at all. A good example of this is the Maersk Lines. They made a decision in 2009 to stop shipping through the Suez Canal and start shipping around the Cape of South Africa to prevent attacks by the Somali pirates. This results in a longer shipping time but a much more secure route. There are trade-offs between security and speed. This is what supply chain managers get paid to do.

In addition, there are natural disasters that have the same impact on the flow of goods and materials that supply chain managers and supply chain leaders need to take into consideration when planning their supply chains. If the security and preparedness of the supply chain are considered as part of the SCOR Model function of Plan the Supply Chain, companies will be postured for success and customers will be assured of an uninterrupted flow of goods and services.

Discussion Questions

1. Discuss the link between supply chain security and homeland security.
2. Pick a retail supply chain and identify potential supply chain risks.
3. Does supply chain security impact profitability?
4. Why is there a trade-off between speed and security?
5. What are the costs of supply chain security?
6. Is supply chain security a USA unique problem? Why or Why not?
7. What purpose does a process map and process walk have in supply chain security?
8. Why is the Country of Origin a concern from a supply chain security perspective?
9. Would Country of Origin reporting have prevented the problems discussed in this chapter?
10. Why should you be concerned about natural disasters impacting supply chains?
11. How does a global supply chain increase the need for both security and preparedness?
12. Search for government recalls of products, why are they being recalled? What is the link of these recalls to reverse logistics?