THE PENNSYLVANIA STATE UNIVERSITY
SCHREYER HONORS COLLEGE

DEPARTMENT OF SUPPLY CHAIN AND INFORMATION SYSTEMS

A COMPARATIVE ANALYSIS ON SUPPLY CHAIN SECURITY

LILLIAN SWEI
SPRING 2018

A thesis
submitted in partial fulfillment
of the requirements
for baccalaureate degrees
in Supply Chain and Information Systems and Hospitality Management
with honors in Supply Chain and Information Systems

Reviewed and approved* by the following:

Susan Purdum
Senior Instructor of Supply Chain and Information Systems
Thesis Supervisor

John Spychalski
Professor Emeritus of Supply Chain Management
Honors Adviser

* Signatures are on file in the Schreyer Honors College.

ABSTRACT

As the supply chains of companies become more globalized, longer, and more complex, the need to security has increased. The risks associated with transporting cargo from overseas are much greater than that of sourcing from within the country. With these increased risks, companies are now realizing the increasing need to secure their cargo, especially from theft and counterfeits. This thesis will compare the supply chain security of two companies from different industries. The purpose is not only to compare and contrast the two different security programs, but also to discover if the related industry needs to design a supply chain security program. The companies referenced in this thesis are from the retail and pharmaceutical industries.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

Thank you, Professor Susan Purdum, for your guidance and unwavering support throughout this thesis process. Without your help and efforts, this thesis process would not have been so smooth.

I would also like to thank all my contacts at the companies who provided the data and knowledge needed for this thesis. Without all your help, this thesis would not have been possible.

Thank you to the Schreyer Honors College and the Smeal College of Business for all the opportunities, high quality of education, network, and experiences that have prepared me for my professional career.

Lastly, thank you to my family and friends who have provided the mental support I needed to continue writing from one page to the next.

Chapter 1

Introduction

In 2013, just a month before Christmas, retail giant Target experienced one of the most terrifying data breaches in the history of the industry. The hackers stole vendor credentials to enter Target's supply chain and gained access to approximately 70 million customer identity records. As reported by Target, the breach affected profit by more than 40 percent in the fourth quarter of that year and incurred a cost of $61 million in expenses in order to mitigate the impacts of the breach. This incident exemplifies the damage and impact an insecure supply chain can have on any company.

"An approximate 80% of data breaches originate in the supply chain", said Torsten George, former vice president of marketing for Agiliance (now RiskVision), a company that specializes in delivering risk intelligence software to large companies (Mello). An IBM study in 2016 surveyed more than 2,400 IT and cyber security professionals around the world and 66 percent of these participants reported that their organization would not be capable of recovering from a cyber-attack ("IBM Study"). The study also showed that more than 70 percent of these organizations are still trying to resolve attacks from one year ago. This shows that these attacks have a lasting impact on these organizations and take months and even years to resolve at a great financial cost.

While data breaches can cause a substantial amount of financial damage, there are other risks that can greatly affect a company's bottom line. These risks include cargo theft, a major problem for many companies. According to a data compilation regarding cargo theft from thirty states in 2016 by the FBI, trucks and trailers are among the top stolen properties with over $6 million in value stolen ("Cargo Theft"). The data shows that security breaches such as cargo theft are a major risk factor that companies should take seriously (see Appendix A).

As supply chains today become more globalized, longer, and more complex, the need for supply chain security is proving to be a growing, important field of study. Supply chain security is a

combination of traditional supply chain management principles combined with security measures against theft, counterfeit, and terrorism. One could argue that supply chain security has four dimensions: product, information, money, and logistic systems (Pope). A breach of any one of these dimensions can be detrimental to a company and consumers it serves. A breach in the product, could mean that the customer did not receive the correct item ordered or no item at all. In some circumstances, such as in the pharmaceutical industry, a product breach can be life threatening as an incorrect drug can cause death (Pope). If information and money is breached, confidential personal information such as credit card and social security numbers are obtained by hackers, putting the consumer at risk. Such a breach always decreases the consumers' trust with the company and hurts the company's reputation. The Target data breach is a perfect example of an information breach. Lastly, a logistics system breach endangers the transportation process of the supply chain itself. Especially with transportation already being one of the major cost centers in the supply chain, having breaches in security with product theft along the way can add additional cost for the company. A retail company loses approximately $60 million a year due to inventory shrinkage, otherwise known as employee theft (Leinbach-Reyhle). Simply put, without supply chain security, any supply chain would be at risk for various incidents that would affect the bottom line for any company. As international business becomes more prominent and more industries source from suppliers overseas, it is more important now than before to make sure that the supply chains are secure to ensure maximum profit and customer satisfaction.

Within supply chain security, track and trace is an area that ensures the visibility in the supply chain and therefore improves the security. While track is responsible for the current and downstream visibility of the supply chain, trace is responsible for the upstream. Tracking is when a company is able to know where a product is in the supply chain at all times. Tracing is the ability to retrieve past knowledge of where the product came from (Koh). The two functions are essential in the supply chain network because it provides the information to answer the questions of when and how a product arrived

at its destination. This way, if there is an incident where a product is missing during the transportation of the product, it is possible to trace where the product was last seen and which individuals interacted with the product.

This thesis will focus on two companies in drastically different industries and the security in each of their respective supply chains. First, each company's finished goods supply chain will be mapped. Then, an analysis of the mapped supply chain will detail how security and trace and trace is integrated. Lastly, the two companies' supply chains are compared with an emphasis on their supply chain securities. An in-depth look into how future technology and processes can help improve each company's supply chain security will also be given. The first company, (disguised as "Company A" for the entirety of this paper) is a leading apparel and personal care items company with several brands under its name. The second company, (disguised as "Company B" for the entirety of this paper) is a large pharmaceutical company that has great domestic and international presence. This comparison will expose how different industries incorporate security into their supply chain and how security in supply chains differs from industry to industry.

Chapter 2

Literature Review

Before discussing the specifics of supply chain security in relation to each company, it is important to first understand the history and current state of supply chain security. This will provide a holistic view of the problem and make it easier later to understand the further implications of the supply chain security systems in their respective industries.

History

The history of supply chain security is rooted in the history of supply chain management itself. Supply chain management was always critical to any business but it was never identified as an individual field until around the 1980s ("A Look Back"). It was around this time that products became containerized to lower transportation costs and the term "supply chain" was coined in 1982 as a result ("A Look Back"). From this point on, the supply chain became a key indicator of a business's success. At this time, however, businesses used the word "logistics" more commonly than "supply chain". Business saw logistics as more of the functional aspect of supply chain and was therefore given more importance. In a 1998 definition of supply chain by the Council of Logistics Management, logistics is "that part of the supply chain process that plans, implements, and controls the efficient, effective flow and storage of goods, services, and related information from point-of-origin to the point-of-consumption in order to meet customers' needs" (Lambert). From this definition, logistics was considered more important than the informational component of the supply chain. The functional, or physical movement, was more important to the business since it drives product sales that translates directly into revenue. it was the driver for sales of the product that would translate into revenue. Even The Pennsylvania State University's Department of Business Logistics was established first in 1989 before evolving into the Department of Supply Chain and Information Systems in 2002 ("A Look Back"). The Pennsylvania State University's decision to broaden its focus and supply chain mission is a

perfect reflection of the industries' needs ("A Look Back"). With the change from logistics to supply chain, more possibilities opened up for the field. Instead of being primarily dominated by logistics and being a "functional" field, supply chain now consists of the flow of information as well (Lambert).

Supply Chain Management

Of the many definitions given, supply chain is best summarized by the definition given by the Supply Chain Council: supply chain encompasses all activities from planning, sourcing, making, to delivery of a product. From this definition, supply chain management is therefore the alignment of the company's goals to deliver to the end consumer. With the trend of companies being reluctant to vertically integrate, the importance of supply chain and supply chain management has become greater than before (Lummus). Instead of vertical integration, companies are seeking out cheaper suppliers in order to cut down on costs (Lummus). It is exactly this phenomenon that increases the need for security within the supply chain.

The Integration of Supply Chain Security

Supply chains today are growing to be more complex domestically and are also extending internationally. The future of business lies internationally using global suppliers, transportation providers, etc. to reach the local customer base at the foreign country. As products and information in a supply chain are making their way not only domestically but internationally, the need to secure the physical and intangible valuables increases.

After 9/11, companies needed to accept the fact that securing their supply chains against terrorism and other threats was no longer an option but a necessity. Everything from accidents to planned robberies happen unannounced and companies need to be sure that they are ready to face whatever challenges hinder their flow of products to the end customer. Professor James Rice of the Massachusetts Institute of Technology's Integrated Supply Chain Management Program defined four levels of initiatives that categorize a company's security efforts. The initiatives are:

Basic Initiatives: First level of security measures that include basic cyber security, physical security measures (camera systems), personnel security (access cards), standard risk assessment (floods, vandalism, etc.), and a basic continuity plan for supply.

Reactive Initiatives: Second level of security that are in place to react to react to supply chain related risk including analysis of supply base to obtain a deeper understanding of how suppliers would behave during events of supply disruption. Most of this level of security was added after 9/11.

Proactive Initiatives: Third level of security includes outside organizations such as law enforcement that could support the supply chain security measures in times of need. This level of security created a new role, Director or Chief of Security, in charge of obtaining the resources needed to maintain security within the supply chain.

Advanced Initiatives: Highest level of security that anticipates possible supply chain risks and will establish drills and simulations to teach employees how to respond during those times. A thorough emergency plan is also in place with procedures to guide individuals through an unexpected interruption.

Unfortunately, according to Professor Rice and his research, most companies are in the lowest level of security, making them vulnerable to the many possible threats that todays' supply chains face.

Pharmaceutical Supply Chain

The pharmaceutical industry is one of the most highly regulated industries by the government in any country. In the United States, the federal Food and Drug Administration (FDA) has strict guidelines on the manufacturing, labeling, and selling of drugs and medical products. In many ways, the governments' regulation is a natural form of security on these drug products for the end consumer. However, this does not stop the amount of drugs that are counterfeited and stolen each year. The World Health Organization (WHO) estimates around five to eight percent of all drugs in the world are counterfeit. WHO has termed the phrase "substandard and falsified (SF)" to refer to all counterfeit

medical products and drugs. “Substandard” products do not meet both or either of their quality standards and specifications. An example of a substandard product would be a medicine that does not contain the amount of active pharmaceutical ingredient that it should. “Falsified” products are those that were deliberately altered but still claims to be the true product; mislabeling is an example of falsifying a product (“Definitions”). Roughly, 120,000 people die a year due to counterfeit malaria drugs in Africa alone (Wall). As for the pharmaceutical companies, not only are they losing sales due to these counterfeited drugs, but these illegal actions affect their reputations as well.

The pharmaceutical industry is currently using auto-ID technology such as RFID tags to authenticate drugs and for track and trace. This is a step up from using just barcodes since they can only be scanned when in visible sight (Koh). Barcodes are applied to each drug bottle or container and, in many cases, the bottles are packed in inner packs within a larger case. Even though the larger cases often have a barcode, that is not enough to be absolutely certain that the case contains the correct inner packs with the validated drugs. Therefore, attaching a RFID tag to the inner case packs would allow better drug integrity and validation.

Fashion Supply Chain

Speed and agility define the fashion industry’s supply chain. Products are constantly being introduced and retired as seasons, trends, and company priorities change. In order to win the market, the supply chain needs to be responsive and be able to deliver at a short time’s notice. The current leading company in this industry is Zara, which leverages its real-time data collection to deliver to stores twice a week in order to meet demands (Shannon). Zara’s vertical integration strategy has allowed it to have control of what is being designed, manufactured, and shipped to stores. Manufacturing 60% of their own products, Zara has great visibility of their supply chain since the connection between manufacturing to retailing is owned by the company itself and little is outsourced. In a way, this is also Zara’s way of protecting its supply chain and increasing its security. With no external, third party involvement, risks are lower and Zara can be more confident in the integrity of their products. Instead of using RFID as just a

security feature, Zara uses it as a way to track which products have been scanned the most, which then indicates the top sales. Zara then effectively uses this information to increase production of a certain product or make other similar products (Shannon).

The retail industry is also one of the most vulnerable industries in terms of security. With an estimated $450 billion value of counterfeited goods in the global market, retail industries are in a constant battle with counterfeiters trying to steal their revenue and taint their reputation (Shannon). Inventory shrinkage, or employee theft, also causes $60 billion in losses for United States retailers (Leinbach-Reyhle). With these unnecessary losses and expenses, having a secure supply chain is crucial for the retail industry.

Emerging Technology in the Supply Chain

Auto-Identification technology, such as with RFID tags, is currently used by most large companies to track their products through the supply chain. However, the future of supply chain technology is said to lie in blockchain technology—the same technology that the crypto currency Bitcoin uses. It is based off the idea of a public ledger where every transaction creates a "block", which are all chained together. A network of users surrounds a blockchain. Everyone in the network must validate a transaction. Once validated, the transaction cannot be changed or altered ("Blockchain 101"). This aspect is where the strength of the technology lies. Even if one node or member of the network is hacked, the information is still safe since the hacker is not able to alter or add transactions as it would require the verification of every node in the network. Members of the network hold a private key for their own identity and a public key for every other member in the supply chain. Both keys are needed to add a transaction. This added complexity along with the distributed network is what potentially makes blockchain the future technology for real-time tracking, validation, and anti-counterfeit prevention.

Recently, Walmart and other food retailers have collaborated with IBM to trial blockchain technology on their food supply. The first trials have proven to be a success as Walmart reported the

ability to instantaneously trace the history of two mangos, which was a process that used to take days (Hackett). Especially for industries that have perishable products, such as food, blockchain technology is an attractive solution that offers the ability to quickly obtain and maintain critical data related to the product. The applications for blockchain technology are endless and industries are already exploring the uses and possibilities.

Chapter 3

Company Backgrounds

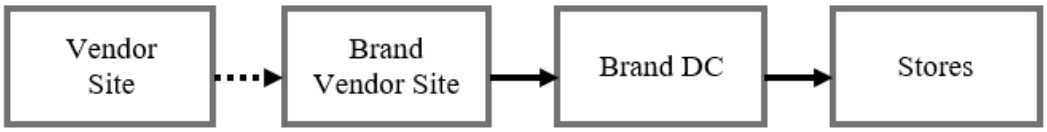
Company A has several brands that encompass high-end apparel to personal care products and luxury handbags. With its recent expansion into Asia with its apparel brand, Company A is quickly gaining international presence. Company A competes with its diverse product mix and its agile supply chain and has established itself as a top company in the retail industry.

Company B is a world-renowned pharmaceutical company with brands for over the counter (OTC) drugs as well as vaccines and oncology drugs. The company sells its products in the Americas, Europe, and Asia in more than 90 countries. Company-owned manufacturing facilities are also located at those regional locations. Company B also produces two of the top leading global OTC drugs.

Company A Finished Goods Flow

Finished goods inventory passes through three different systemic sites before reaching the store/ consumer level.

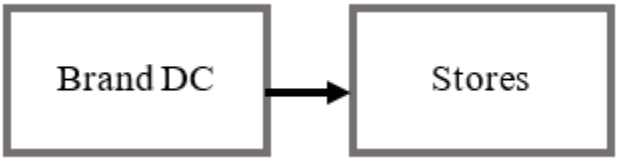
Figure 1. Company A Inventory Flow Map



At Company A, the Vendor Site and Brand Vendor Site are systemically different sites but physically the same location. The financial ownership then transfers between the systemic Vendor Site and Brand Vendor Site. Once production hits the Brand Vendor Site, financial ownership transfers to the brand. For the purpose of analysis, Branch 1 is defined as the flow of inventory from Vendor Site to Brand Vendor Site to Brand distribution center (DC). Branch 2 is defined as the flow from Brand DC to Stores.

Figure 2. Company A Branch 1

Figure 3. Company A Branch 2



Flow of Inventory from Vendor Site to Brand Vendor Site to Brand DC: Branch 1

Company A outsources the entirety of its manufacturing to third-party vendors. Because of this, the idea of brand protection becomes very important. With vendors located around the world, protecting the image of the brand becomes a challenging task. Company classifies vendors as either managed vendors or turnkey vendors. Managed vendors receive components or certain raw materials to make the product. These components are usually branded with Company A's brand logos. Therefore, it is important that products with these brands are not leaked out of the supply chain network. Turnkey vendors purchase their own raw materials and Company A only buys the finished good. Even so, the finished good is most likely marked with a brand logo that belongs to Company A. Constantly monitoring the vendors and verifying the products with company labels are properly produced, shipped out, and (if necessary) destroyed is of utmost importance when it comes to protecting the company's image.

Security of Inventory Flow in Branch 1

Company A has been predominately concentrated its business in North America until around 2011 when it started expanding to Canada and overseas. This makes Company A a fairly new player in the international business space; with this came many challenges in order to establish an effective supply chain security process with approximately 400 vendors located globally.

Cases and issues are usually put in one of the four categories:

Table 1. Case Categories

Case Category	Description
Counterfeit	Illegal imitation of product
Diversion	Product is leaked out of the supply chain at vendor
IP infringement	Intellectual property or trademark infringement of the company's brands
Grey Market	Product that was sold to channels not intended for

There is a clear distinction between each of these categories though they seem similar. Counterfeit goods are created completely out of the supply chain network of the company while diverted goods originate from the network itself. Intellectual property (IP) infringement encompasses illegal use of Company A's trademark. The most common case of IP infringement is the opening of Company A's brand stores without permission. Lastly, grey market cases occur when a retailer intentionally sells product into a unintended channel. The key difference between diverted products and grey market products is the point at which products leaves the supply chain. Diverted products leaves the supply chain at the vendor while grey market products leave at the retailer stage. This can happen if a retailer who has permission to sell Company A's products purposely orders more products to sell in bulk to another, unauthorized retailer. Though each one of these case categories presents its own unique risks, Company A has created a process to prevent these incidents early on.

In order for the company to have any legal power to interfere and terminate any of the case categories above, a trademark portfolio must exist for the company's products at the country where the issue exists. Trademark portfolios are broken down into a class for each unique product type and each product type must have a portfolio addition request for each country. The more brands, products, and countries where the products are sold exists for a company, the larger and more complex its trademark portfolio will be. For example, if Company A sells innerwear (bras, panties, and underwear) as well as outerwear (shirts, jackets, pants, etc.) and these two products type were two separate classes, two requests would have to be made to have these added into Company A's trademark portfolio for a one country. If in

the circumstance that a theft was to occur at a country where the product stolen is not part of the company's trademark portfolio, Company A would have no legal power to investigate the incident and can only take on the financial damage of the incident. The first step into having a secure global supply chain would be to have a well-covered trademark portfolio for every product type in every country the company engages in business.

Areas of Audit

Company A has seven areas of audit at the vendor level that serve as layers of prevention. The areas of audit are:

Table 2. Areas of Audit

Area of Audit	Definition
Photo	Photo of finished product cannot be leaked before the product is launched
Sub-Contracting	Monitoring of any work that is sub-contracted to complete the product (ex. printing, dyeing, etc.)
Sample	Quality control of samples of the product
Componentry	Monitoring of components that were provided to complete the product
Destruction	Componentry or any other material that has the company brand logos must be properly destroyed as specified
Finished Goods	Finished goods must meet pre-determined specifications
Customs/ Regulatory	Vendor must comply to laws where they operate (ex. labor standards)

These seven areas of audit not only keep the vendor compliant with all of Company A's standards but it also helps to minimize incidents that would later fall into one of the case categories. The first area of audit, photo, mainly affects counterfeit. Counterfeits are more likely to occur if photos of the product were leaked before the release of the product. Of the seven areas of audit, destruction audit has a great impact in preventing downstream product security incidents. Any product that contains any of Company A's brand logo that is not intended for sale must be properly destroyed in order to minimize the risk of counterfeit and diverted goods.

Brand protection has a broach range of responsibility from before the manufacturing of the product to after the finished good is produced and to the brand's DC. Brand protection is more concerned with the legal compliance of all the incidents than the financial impact. It is their ultimate responsibility to ensure the integrity of the brand to its consumers.

Flow of Inventory from Brand DC to Stores: Branch 2

While inventory flows from site to site in Branch 1 on the pallet level, inventory flows from the Brand's DC to the Stores on a carton level. Here, the idea of asset protection is more prominent. In Company A's network, there are multiple DCs spread across the United States. A dedicated team is responsible for placing allocations to the store level from these various DCs. Once allocations are made, a trailer load of allocations departs for a third-party delivery agent that is located near the stores where the allocations are due. It is at the delivery agent where the trailer load is broken down into smaller truckloads to depart for the individual stores.

Security of Inventory Flow in Branch 2

Another dedicated team ensures the security of products at Company B that flows from the Brand DC to stores. This team focuses on two aspects of the flow: products and people.

Products

Company A has a large product mix but all the products have one commonality—small size. Beauty and apparel products are all packaged in a box that contains several quantities of the same product and are, therefore, easy targets for theft. In the industry, this is referred to as shrinkage, or theft that occurs in the network before the product reaches its final destination. Shrinkage directly affects the bottom line of a company and can be significant if not prevented against immediately.

The link from the delivery agent to the stores is the most vulnerable to theft in this branch of the finished goods supply chain. Small vans making store delivers usually hold several boxes of different

types of product per van. With high value products ranging from $40 to $80 per piece, a box can easily fit at least six of each product. One stolen box can lead to more than $500 of revenue losses. Therefore, proper prevention and reaction practices must be established to detect, mitigate, and eliminate these thefts as quickly and efficiently as possible.

In one occurrence, a gang was targeting one of Company A's brands' vans and clearing out all the contents of the van while the driver made trips unloading the van at the store. This led to a full-fledged investigation where eventually the culprits were caught. However, the most valuable piece of information Company A learned from this incident was about the tool the thieves were using the break the lock on the vans. Company A's asset protection team was then able to test out several locks to see which could withstand the tool. The outstanding lock was then fitting on all the vans of the delivery agents partnered with Company A that would contain the high value products. The amount of thefts significantly decreased after this increased protection. Company A was able to use the incident to their advantage by better protecting their products with information learned from the event.

People

As the number of touches on a product increases, the risk for the product increases as well. This statement holds true for all supply chains as nodes and complexity are added. When a trailer load of product is sent to the delivery agent to be broken down, it is an added touch in the supply chain. Firstly, the driver of the trailer is a risk to the average $1.2 million price tag of each trailer. There have been cases where the driver would stop at private storage facilities to unload, and therefore steal, part of the trailer load. Cargo thieves would also tail trailers that leave the distribution center and break into the trailer at rest stops. In prevention of these behaviors, Company A made it a policy for trailer drivers to not stop for 150 miles after leaving the distribution center. Company A also evaluated all of the truck stops in the country and high-risk stops were identified. Each truck is equipped with a card that lists all high-risk stops and if a driver decides to stop at one of these stops and product is lost, the carrier is fully liable for the load.

Once the trailer makes it to the delivery agent, employees are another source of risk. Cartons can easily be intentionally left out and stolen when breaking down the larger trailer into smaller vans for store deliveries. The van driver then poses the next threat. Here, a similar risk to the trailer driver exists but there is also an additional risk where the driver can systemically deliver the product to the store but physically leave it in the van and steal the product. This can be very difficult to detect since the store has to report the theft first for it to not count towards its performance. Therefore, in prevention of such incidences, Company A conducts very thorough background checks on all employees that will be directly in contact with the products.

Another preventive method Company A uses to determine the risk exposed to their product is through GPS tracking. Each year, an analysis is done to determine the highest risk stores, delivery agents, and individuals. GPS tracking devices would then be put in loads that would be in contact with these high-risk nodes to monitor the risk. By constantly testing and evaluating the risks in the supply chain, Company A is able to more quickly detect and react to incidents and make the right decision to prevent them in the future.

Human Resource Support

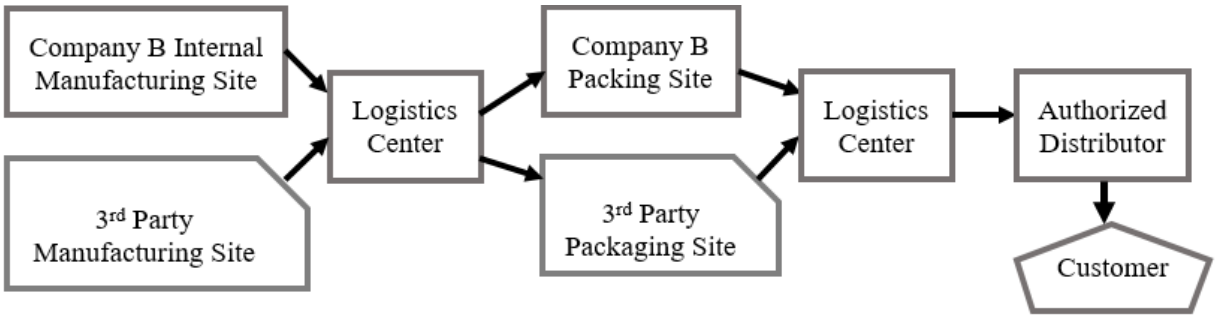
Company A has two teams of tightknit individuals who each specialize in either loss prevention or brand protection. Loss prevention is primarily concerned with managing the goods that are in North America. Any incidents related to stolen or damaged goods in North America are reported to loss prevention and it is their responsibility to investigate. This team is mainly based in the United States and works to minimize risks such as cargo theft. Loss prevention’s efforts are reported to the Chief Financial Office (CFO) as the risks will directly impact the bottom line. On the other hand, brand protection works closely with the legal team to ensure that individuals without permission do not misuse the company's brands. Brand protection has associates located around the globe closely monitor each region.

Chapter 4

Company B Finished Goods Flow

Being in the pharmaceutical industry, the finished goods supply chain flow of Company B is very complex, intricate, and involved. With a combination of internal (owned) sites and external (3rd party) sites, Company B is required to have high visibility of their product as it moves through its supply chain through different financial ownerships and responsibilities. With a combination of internal and external sites, the amount of risks and number of touches also greatly varies based of whether or not the product is made internally or externally.

Figure 4. Company B Inventory Flow Map



In other words, the final finished goods move through the supply chain in five stages before reaching the end customer. External involvement can be found at almost every stage. However, this is only the general map of the supply chain at Company B. With more than 24,000 SKUs in over 170 markets, this is only one aspect of the company's complex supply chain. The chain also includes 64 internal manufacturing sites and 134 logistics centers. Depending on the type of product, whether it is an OTC drug, a prescription drug, R&D drug, and so on, the supply chain of the product may vary. This creates multiple types of supply chains within the company each unique with its own set of nuances and challenges. Also with the manufacturing sites located around the globe, the amount of variability and exposure to risk increases as well. As the complexity of the supply chain increases the difficulty to secure each unique supply chain increases as well.

Securing the Supply Chain: Prevention and Detection

There are four areas of risks that Company B's supply chain security team prioritizes. These four areas are counterfeit, diversion, cargo theft, and intentional adulteration. Company B has come up with seven key focus areas that will prevent the four key areas of risk.

Table 3. Focus Areas

Focus Area
Influence the External Environment
Supply Chain Security Regulation Implementation & Compliance
Globalization
Enhancing Supply Chain Transparency & Control
Continuous Improvement
Competitive Advantage
Education & Industry Collaboration

The first focus area of "influence the external environment" is the best representation of preventing and detecting areas of risk. This focus area pertains to working with external groups that are able to dictate and influence the flow of the products. These groups include the FDA (Food and Drug Association) in the US and the FMD (Falsified Medicines Directives) in Europe. By escalating the problem to the governmental degree, Company B is able to increase their reach in the problem. For example, one of the detection methods that Company B is striving to enforce is the track and traceability of products as it moves through the supply chain. They even developed an app that helps their own associates track the status and location of a shipment as it moves through the supply chain. If it becomes a legal requirement, vendors are then obliged to comply which will greatly reduce the risks of the products in the supply chain. Governmental influence would also set a global standard for other countries to comply. The second area of focus aims to implement and enforce these regulations and increase compliance within governments of other countries and their manufacturing sites. The third focus area of "Globalization" ties together the first and second focus areas. It is necessary to prevent and detect areas of potential loss revenue from a global standpoint due to Company B being a highly globalized company.

"Enhancing supply chain transparency and control" and "continuous improvement" focus areas further enforce the importance of implementing and enhancing track and trace technologies. This increases supply chain transparency, which strengthens supply chain reliability and decrease risks. Supply chain transparency allows for greater visibility into where each product is at all times in the supply chain. In the event that an incident occurs, it is easier to track down which products, at what quantity, and to what degree the negative impact of the incident. From these six areas then creates a competitive advantage for Company B that they can use to leverage further industry collaborations and opportunities to educate other organizations in the pharmaceutical industry in the field of supply chain security.

Leveraging Governmental Programs for Security

Company B demonstrates effective use of governmental and international programs to enhance their supply chain security measures. One of these governmental programs is the Customs- Trade Partnership Against Terrorism (CTPAT). This program was developed in response of the 9/11 and ever since the United States Customs and Border Protection department has been more concerned about upstream supply chain activities than ever before. Pre 9/11, the Customs and Border Protection would only look at the goods that were imported for risks. Now, they also check the source of the shipment and analyzing the risk of the supplier and the country the shipment originated. This is because the United States became wary of weapons of mass destruction or components for weapons of mass destruction to enter United States soil. As a result, companies importing from suppliers overseas are greatly impacted. This initiative translates into elongated wait times in customs once a shipment arrives in the United States. Therefore, companies began to react to this change by joining the CTPAT program. This is a voluntary program where companies demonstrate to the U.S. Customs and Border Protection department that as a company, they are low risk and cooperate with their suppliers, transportation providers, manufacturers, etc. to lower these risks and enhance the safety and security of products that are being imported into the U.S. under their company's name. In return, the company enjoys expedited customs

screenings and has their goods released sooner compared to companies who are not CTPAT certified. Also, by collaborating with other companies who are CTPAT certified further decreases the risk of having the shipment held at customs for inspection.

The process of becoming CTPAT certified is considered a cost or investment depending on the company but it does require a lot of planning and coordination throughout the entire supply chain. The U.S. Customs and Border Protection wants to see several forms of documentation including a risk assessment and a supply chain security profile. By having elevated entry requirements, the U.S. Customs and Border Protection is ensuring that the companies who participate are those who have a strong supply chain security able to meet the requirements and add to the initiative of strengthening security in the international supply chain.

Company B happens to not only be CTPAT certified by also has certifications in other programs including the Certified Cargo Screening Program by the Transportation Security Administration, Secure Supply Chain Pilot Program run by the Food and Drug Administration, and Partners-In-Protection, a Canadian Initiative. The benefits of these programs outweigh the process of obtaining the certification for Company B. As a pharmaceutical company, much of Company B's inventory is perishable medication that needs to reach the end consumer as soon as possible. Therefore, it is crucial to minimize any sort of delay that impacts this delivery. By going through the rigorous process of becoming certified, Company B saves themselves time in the future when it is critical to deliver a certain shipment by a predetermined date.

Company B is also effective in leveraging these certifications to ensure and encourage suppliers and third party transportation providers to have proper security measures as well. By securing the supply chain early on, it decreases risks as the product moves further down the supply chain. Being the pharmaceutical giant that they are, Company B has the power to influence their suppliers and logistic providers to comply with their initiatives. In return, this will increase the security of the supply chain as a whole.

Securing the Supply Chain: Reaction

Having strong risk assessment and detection plan is as important as it is to set procedures in place that guides reactions to supply chain security issues. Company B has a detailed standard of procedure (SOP) that documents the responsibilities of each logistics branch that is impacted by an unplanned incident. The process works similarly to that of a decision tree. Each branch has a set of actions that corresponds to the state of the incident. The SOP document also provides the names of who to contact depending on the region of the incident originated from. Having such a standardized method of reacting to situations has many benefits. It ensures that every incident is documented and addressed as quickly as possible and by having a centralized database for incidents; it also verifies that incidents are not duplicated. Company B thoroughly prepares themselves through multiple layers of prevention practices to minimize the number of unplanned incidents. However, these incidents may also include those that are a result of natural disasters. Because Company B is a pharmaceuticals provider, an SOP is important for two reasons: first, Company B needs to deliver medication to the hospitals and organization in need that are treating victims of the disaster, and secondly, Company B needs to expedite their import of supply to meet the demands. It is especially critical to have a SOP to respond quickly to incidents that occur during these times.

Human Resource Support

It would be nearly impossible for only a few teams of people to support such a large and complex supply chain even without factoring the security variable. Company B's supply network is supported by over 34,000 associates who work together to manage the supply and therefore helps to enhance the security of the products. A dedicated department to supply chain security then helps to ensure that all the preventive, detective, and reactive procedures are up to date. The department is also responsible for investigating the incidents that arise with teams dedicated to the type of problem whether it is theft,

counterfeit, etc. This highly specialized way of segmenting the supply chain allows for detailed monitoring of the company's supply at all stages through its supply chain.

Chapter 5

Analysis: Compare and Contrast

Intent for Security Program

Each company has a different motivation for implementing a supply chain security program. This motivation then shapes the growth of the program and influences how the company will continue to strengthen or maintain the security in their supply chain. Company A, being a retail company, was motivated by the amount of thefts of their products they saw in their supply chain. In effort to reduce these risks and financial losses, Company A looked to better secure their supply chain, and it was effective. Theft rates have dropped compared to 10 years ago even in the areas that are considered high theft risk in the United States.

Company B's motivation is more complicated than that of Company A's. As a pharmaceutical company, Company B has to ensure the integrity and safety of their products, and prevent any counterfeits emerging outside of their supply chain. In addition, because pharmaceutical companies are more regulated in nature, Company B has to comply with more product regulations which naturally makes sense for them to initiate a security program. Here, the security program is an investment that would contribute to mitigating the risks and compliance factors that Company B would have to face regardless. Therefore, this greatly influenced Company B's supply chain security growth. By participating in governmental programs, Company B not only established further credibility with the government but also contributed to their own supply chain security goals and standards. As Company A's international business begins to grow and their level of imported goods increases, this is also a strategy that Company A can consider taking to further enhance the security of their supply and suppliers and decrease the amount of time it takes to import goods into the United States.

Measure of Effectiveness of Supply Chain Security

With different motivations of implementing a supply chain security program or function, each company also has different ways of measuring the effective of the program or function. For Company A, the measures are more straightforward, it can be easily seen in the numbers of the cargo thefts and dollar values of the thefts. The security measures have been effective if these numbers decrease over time and, fortunately, they have been. As for a measure of effective for brand protection would likewise be if the numbers are decreasing in the number of unauthorized stores and illegal uses of Company A's brands, it is an indication that the function is performing their job well. Supply chain security is a way to reduce cost and protect the brand.

However, with Company B, these measures become a bit more complicated. With supply chain security more integrated in the supply chain process itself, Company B's measures lie within improving or enhancing the efficiency of their supply chain. Company B uses supply chain security as a competitive advantage against other pharmaceutical companies. To a certain extent, it is a requirement but it is more a strategic plan that increases the efficiency of their supply chain. By strategically choosing suppliers who are also certified in security programs, Company B is using their security measures to ensure the efficiency of their supply chain downstream. Therefore, measures such as number of thefts, counterfeits, trade infringements, etc. still apply but there is an added layer of how supply chain security relates to the fluidity of the supply chain as a whole. The supply chain process should not be interrupted due to security and risk issues. All of these threats are evaluated beforehand and constantly monitored to ensure the goods are transported safely and as little disruption as possible to their final destination. Company B's supply chain security adds value and supports their strategic and operational goals. In short, Company A's measures focus are rooted in numbers and the bottom line impact that the security initiative can make while Company B's measures expand deeper into the supply chain.

Potential Implementation of Blockchain Technology

Both Company A and Company B could benefit greatly implementing blockchain technology. The technology would enhance inventory integrity with its shared public ledger characteristic that would help to easily quantify in the shortest amount the impact of cargo theft. The technology would also lead to a decrease of counterfeit products since all products are confirmed and an unverified product would be easily identifiable. Especially for Company B, being in the pharmaceutical industry, this is especially important. Counterfeit drugs can easily destroy the company's reputation and can cause health concerns. As for Company A, blockchain technology can help identify weak points in the supply chain to prevent against cargo theft. However, in terms of readiness, Company B is better equipped with the resources that would better support the technology. Company B has a very clearly established supply chain security program with the people needed to support its complexity. The company has also created a supply chain tower that houses the data necessary to support the supply chain. Therefore, from a technological infrastructure and human resource standpoint, Company B is better equipped to implement a technological system such as blockchain.

Chapter 6

Conclusion

Company A and Company B have both demonstrated that in order to implement a successful supply chain program, having the necessary human resources is of first importance. Secondly, both companies have also exemplified that a supply chain does indeed differ based on the nature of the industry. The industry needs motivate the company to design and implement a supply chain security program. Therefore, a supply chain security program is never one-size fits all but is catered to the specific industry and company it is designed and created for. Company A's supply chain security, being in the retail industry, is more focused on cargo theft, and brand protection. While Company B is also concerned with these security measures, they also prevent against counterfeit due to being in the pharmaceutical industry. Supply chain security is a highly adaptable aspect of the supply chain that can be designed to fit any supply chain.

Limitations of Research

Due to fact that only two companies from each industry provided data, the information provided is limited to what was provided by the two companies. Therefore, the facts may be biased towards how these two particular companies designed their supply chain security program. The other limitation would be the lack of access to numerical data to conduct a quantitative analysis. A quantitative analysis would have provided more insight into the effectiveness of each of the supply chain security program. Having access to data such as the number of thefts and counterfeits as well as what the security program did to decrease those numbers would have been beneficial.

Suggestions for Further Research

To further improve this research, a larger sample population of companies is suggested. By increasing the number of companies in each industry and increasing the number of industries, a more accurate conclusion can be reached on whether or not supply chain security is dependent on the industry.

Other industries to include in the study may be manufacturing, consumer electronics, oil/gas, etc. These industries all have high final goods costs that would benefit from a well-designed supply chain security program.

Appendix A

Cargo Theft Data from 30 States

Cargo Theft Property Stolen and Recovered by Type and Value, 2016			
Type of property	Value of Stolen Property	Value of Recovered Property	Percent Recovered
Total	**$26,933,356**	**$8,449,949**	**31.4**
Other	6,770,506	1,021,466	15.1
Trucks	3,919,445	2,879,963	73.5
Consumable goods	3,066,939	301,116	9.8
Trailers	2,589,730	1,735,703	67.0
Household goods	1,557,553	112,920	7.2
Building materials	1,262,488	441,583	35.0
Portable electronic communications	1,262,051	18,185	1.4
Metals, nonprecious	1,126,825	952,500	84.5
Alcohol	826,360	1,029	0.1
Merchandise	732,734	27,568	3.8
Computer hardware, software	530,772	515,925	97.2
Radio, TV, VCR	472,001	1,500	0.3
Automobile	392,879	180,000	45.8
Clothes, furs	390,666	5,420	1.4
Tools	379,657	21,850	5.8
Industrial equipment	371,693	52,183	14.0
Vehicle parts	345,766	69,334	20.1
Office equipment	303,062	0	0.0
Other motor vehicles	122,700	60,000	48.9
Livestock	120,000	0	0.0
Recreational, sports equipment	100,500	0	0.0
Photographic, optical equipment	53,100	2,800	5.3
Drugs, narcotics	50,081	0	0.0
Firearm accessories	41,200	40,000	97.1
Money	35,029	0	0.0
Fuel	29,770	0	0.0
Chemicals	20,400	0	0.0
Jewelry, precious metals	17,768	548	3.1
Firearms	15,550	3,650	23.5
Musical instruments	9,000	0	0.0
Bicycle	6,527	0	0.0
Lawn, yard, garden equipment	5,406	4,206	77.8
Farm equipment	3,368	500	14.8
Purse,wallet	959	0	0.0
Medical, medical lab equipment	702	0	0.0
Camping, hunting, fishing equipment, supplies	144	0	0.0
Negotiable instrument	15	0	0.0
Pending inventory	10	0	0.0
Credit,debit cards[1]	0	0	
Identity documents[1]	0	0	
Nonnegotiable instrument[1]	0	0	
[1] According to Uniform Crime Reporting guidelines, the value of property stolen and/or recovered must be zero for this property description.			

(FBI, 2016)

BIBLIOGRAPHY

"A Look Back..." Penn State Smeal Supply Chain Program, www.smeal.psu.edu/cscr/documents/a-look-back-penn-state-smeal-supply-chain-program+.

"Blockchain 101." Blockchain 101 Infographic, IBM, 30 Jan. 2018, www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=XI912346USEN&.

"Cargo Theft." FBI, FBI, 8 Sept. 2017, ucr.fbi.gov/crime-in-the-u.s/2016/crime-in-the-u.s.-2016/additional-publications/cargo-theft.

"CTPAT: Customs Trade Partnership Against Terrorism." Border Security, U.S. Customs and Border Protection, 25 Jan. 2018, www.cbp.gov/border-security/ports-entry/cargo-security/ctpat.

"Definitions of Substandard and Falsified (SF) Medical Products." World Health Organization, World Health Organization, 2018, www.who.int/medicines/regulation/ssffc/definitions/en/.

Hackett, Robert. "Walmart and 9 Food Giants Team Up on Blockchain Plans." Fortune, 22 Apr. 2017, fortune.com/2017/08/22/walmart-blockchain-ibm-food-nestle-unilever-tyson-dole/?utm_medium=enews_09052017.

"IBM Study: Orgs Not Prepared to Recover from Cyberattacks." *IBM News Room - 2016-11-16 IBM and Ponemon Study Reveals Organizations Remain Unprepared to Respond to Cyberattacks - United States*, 16 Nov. 2016, www 03.ibm.com/press/us/en/pressrelease/51067.wss.

Koh, Robin, et al. "Securing the pharmaceutical supply chain." *White Paper, Auto-ID Labs, Massachusetts Institute of Technology* (2003): 1-19. http://www.adeptpkg.com/wp-content/uploads/2016/09/Securing-the-Pharmaceutical-Supply-Chain_MIT-AUTOID-WH021.pdf

Lambert, Douglas M., Martha C. Cooper, and Janus D. Pagh. "Supply chain management: implementation issues and research opportunities." The international journal of logistics management 9.2 (1998): 1-20. http://ecsocman.hse.ru/data/676/863/1219/article1.pdf

Leinbach-Reyhle, Nicole. “New Report Identifies US Retailers Lose $60 Billion a Year, Employee Theft Top Concern.” Forbes, Forbes Magazine, 8 Oct. 2015, www.forbes.com/sites/nicoleleinbachreyhle/2015/10/07/new-report-identifies-us-retailers-lose-60-billion-a-year-employee-theft-top-concern/.

Lummus, Rhonda R., and Robert J. Vokurka. "Defining supply chain management: a historical perspective and practical guidelines." *Industrial Management & Data Systems* 99.1 (1999): 11-17. https://scholar.google.com/scholar?hl=en&q=supply+chain+history&btnG=&as_sdt=1%2C36&as_sdtp=

Mello, John P. “Target Fiasco Shines Light on Supply Chain Attacks.” TechNewsWorld.com, 3 Feb. 2014, 1:56 PM PT, www.technewsworld.com/story/79908.html.

Pope, James A. "Dimensions of Supply Chain Security." *Southern Business Review*, vol. 33, no. 2, 2008, pp. 21-27, *ABI/INFORM Collection*, http://ezaccess.libraries.psu.edu/login?url=https://search-proquest-com.ezaccess.libraries.psu.edu/docview/228225499?accountid=13158.

Rice, James B. “Rethinking Security.” Logistics Management, Mar. 2007, ctl.mit.edu/sites/ctl.mit.edu/files/library/public/article_Rethinking_Security_LM_May2007_rice.pdf.

Shannon, Sarah. “Fighting the $450 Billion Trade in Fake Fashion.” The Business of Fashion, 2 Mar. 2017, www.businessoffashion.com/articles/intelligence/fighting-the-450-billion-trade-in-fake-fashion.

Wall, Matthew. “Counterfeit Drugs: 'People Are Dying Every Day'.” BBC News, BBC, 27 Sept. 2016, www.bbc.com/news/business-37470667.

ACADEMIC VITA

LILLIAN SWEI

University Park, PA 16802

scyun96@yahoo.com

Education

The Pennsylvania State University, May 2018
B.S., Supply Chain & Information Systems
B.S., Hospitality Management
Minor in Japanese and Korean Languages
Honors in Supply Chain & Information Systems

Thesis: A Comparative Analysis of Supply Chain Security
Supervisor: Susan Purdum

Related Experience

Pfizer Inc. - Collegeville, PA
Global Procurement Intern
May 2017-August 2017

LBrands – Columbus, OH
Supply Chain Planner Co-op
August 2017 – December 2017

Honors and Awards

MIT Supply Chain Excellence Award (2018)
Steward A. Stumpo Trustee Scholarship (2014-2018)
Dean's List (2014-2018)

Memberships/Activities

Tea Institute of PennState
Korean International Club
PennState Learning- Japanese Language Tutor