

DECIDING ON UNCERTAINTY: HOW
SUPPLY CHAIN RISK AND
DECISION MAKING
INTERACT

By

Alexandra E. Kester

Submitted in partial fulfillment of the
requirements for Departmental Honors in the
Department of Supply Chain Management
Texas Christian University
Fort Worth, TX

May 2, 2014

DECIDING ON UNCERTAINTY: HOW
SUPPLY CHAIN RISK AND
DECISION MAKING
INTERACT

Project Approved:

Supervising Professor: Laura Meade, Ph.D.

Department of Supply Chain Management

Travis Tokar, Ph.D

Department of Supply Chain Management

Beata Jones, Ph.D.

Department of Information Systems

ABSTRACT

As the supply chain becomes more advanced, it also opens itself up to more opportunity for risk. Managers need to understand what factors affect risk, how to identify potential risk sources, and decision making strategies to help mitigate risk. Managers also need to understand that risk can occur throughout the entire supply chain, from supplier to customer. This paper will strive to review risk identification and mitigation strategies that will allow managers to start their risk framework. Finally, these strategies will be applied to a consumer packaged goods manufacturer and their customer facing supply chain.

TABLE OF CONTENTS

INTRODUCTION	1
REVIEW OF LITERATURE	3
Vulnerability Points	3
Risk Identification	6
Disruption Severity	11
Risk Mitigation	12
CUSTOMER FACING RISK DRIVERS	18
Data Analytics	19
Applied Framework	21
Results	22
CONCLUSION	23
REFERENCES	24

INTRODUCTION

The supply chain environment is unpredictable and rapidly changing. Companies are under increased pressure to deliver their products faster and reduce costs simultaneously. Current trends in supply chain operations include outsourcing non-core competencies, supply base reduction and lean inventory practices. A study performed by Juttner (2005) identified “globalization, the move towards lean supply and centralized distribution and stock holding were among the most frequently mentioned supply chain strategy elements with severe risk implications” (Juttner, 2005, 133). The overall supply chain is becoming more efficient and removes redundancy from the process. These practices work well in times of normal operation, but what happens when a major supplier has a fire, or a terrorist attack shuts down a key port for good movement? These kind of unpredictable events are supply chain risks and can cause major delays in supply chain operations.

Every supply chain faces risks that threaten its ability to operate efficiently. According to Aven and Renn (2009) risk has two prevailing characteristics, uncertainty and severity of the consequences of an activity. Supply chain risks are an uncertain occurrence that companies encounter, they are hard to predict and plan for. The risks also have different outcomes and impacts to the firm. They may be an isolated incident that only affects one supplier or the risk may shut down the material flow entirely. Juttner (2005) defines supply chain risk as the disruption of information, materials, product or money flows. The relationship between uncertainty and flow disruption is where most

companies get into a bind because their normal operations are not equipped to handle these situations.

The movement towards supply chain efficiency has increased their vulnerability when disruptions do happen (Christopher and Lee, 2004). Many of these risks are not within the control of the company but can cause major disruptions and expense to their supply chain processes. Rice and Caniato (2003) surveyed one firm that estimated the impact of a supply disruption to be \$50 to \$100 million dollars per day. A fire at Toyota's break-fluid proportioning valve supplier, forced the company to shut down 20 assembly lines for six weeks and cost \$40 million per day (Nelson, Mayo, and Moody, 1998). In 2002, the 10 day dock strike in the US, caused 29 ports to be shut down and cost the US economy to lose \$1 billion a day (Simpson 2002). The impact that one event can have on a single supply chain, as in the Toyota case, or on many supply chains, as in the US dock strike, makes supply chain risks and important issue for companies to be monitoring. These disruptions and the costs associated with them are not isolated instances and companies expect the vulnerability of their supply chains to increase, in the next five years (Juttner, 2005).

The research on supply chain risk has exploded in the past several years and has been analyzed from many different perspectives. This paper will study the many facets of supply chain risk from magnitude to mitigation. The Literature review will connect common themes in supply chain risk research including vulnerability points, risk identification, disruption severity and risk mitigation strategies. Each of these areas needs to be understood for companies to identify where potential risks can occur and make

educated decisions about how to handle risk. Currently, there is a gap in the research about how customer actions affect supply chain risk and vulnerability. To examine this, one of the risk identification archetypes will be utilized to categorize stock out codes for a commercial manufacturing firm.

REVIEW OF LITERATURE

Vulnerability Points

A supply chain or supply network is a group of individual entities that connect by flow (Juttner, 2005; Craighead, Blackhurst, Rungtusanatham and Handfield, 2007). There are four things that flow across a supply chain, information, material, product and money (Juttner, 2005). Disruptions occur when any of these flows stops. Identifying the areas that cause flow disruption are determined as vulnerability points in the supply chain. Supply chain vulnerability research has a general consensus that vulnerability is elusive and is influenced by certain characteristics, supply chain design and the supply chain environment (Wagner and Nashat, 2011). All supply chains have different points in their network where vulnerabilities can occur. The evolution of the supply chain to be more efficient has also resulted in increased vulnerability, as supply chain processes have been whittled down to the bare minimum (Choi and Krause, 2005; Stecke and Kumar, 2009; Neureuther and Kenyon, 2009). Recent trends contributing to the slimming down of the supply chain include just-in-time production and LEAN principles. A focus on core competencies leads companies to outsource non-core processes to other organizations. Neureuther and Kenyon (2009) suggest that as companies create flatter and narrower supply structures they have an increased risk of a single point of failure. Identifying the

weakest point in the supply network will help companies pinpoint areas they need to monitor for potential risk.

Points of vulnerability in a supply chain can come from three different sources; the supplier, the firm, or a customer (Neureuther and Kenyon, 2009). The risks center on the disruption of flows, information, material, products and money, between organizations (Juttner, 2005). A disruption in any of these areas can affect that entire network and cause the entire supply chain delays, due to the interdependence of modern supply networks. The major source of vulnerability is from the supplier. Single source, multiple single source and multiple source structures are the three basic kinds of supply chain structure (Neureuther and Kenyon, 2009). No matter what kind of structure a company employs, each firm has a different relationship with each of its suppliers. Choi and Krause (2006) define the supply base as the suppliers that are actively managed by the focal firm. This wide spectrum of supply systems can each lead to vulnerability in the supply chain. A single source strategy leaves the company reliant on only one entity for the materials incoming. The firm then becomes vulnerable to anything that may happen to that source. If something does happen, they have no other incoming material. A multiple single source strategy is similar to a single source, however the firm is trying to get multiple components from multiple single source suppliers. If the firm has a multiple source supply structure they have a large, diverse supply base to manage. If a disruption happens in a large supply base the focal firm may have to deploy resources to help manage the disruption, taking resources away from other suppliers in their supply base. A complex supply base also becomes problematic when a supplier is providing product to

both the focal firm and another supplier in the firm's network. If a disruption happens in a supplier that has this kind of relationship, the focal firm could see ripple effects of that event throughout the supply base causing major delays (Choi and Krause, 2006).

The second major source of vulnerability is the focal firm itself. The practices and management of the supply chain internally can create vulnerability to the organization. One of the major areas that can be affected by disruption is the firm's inventory control method (Neureuther and Kenyon, 2009). As supply chains move toward a leaner model of manufacturing they place increased risk on the availability of inventory if a disruption should occur. In lean and just-in-time inventory models the firm wants to hold very little inventory and use the inventory that they do have very shortly after receiving it. This type of model works well when the supply chain is running normally and the parts are coming in on time, however they are more susceptible to delays if the material flow is interrupted. Firms are also outsourcing many of their non-core competencies which leads to less visibility in the supply chain as a whole. These practices force the focal firm to relinquish control of some areas to streamline the business as a whole. Neureuther and Kenyon (2009) conclude that although this type of structure is more efficient, it is also more vulnerable.

The last part in the supply chain structure where vulnerability can occur is with the firm's customers (Neureuther and Kenyon, 2009). This portion of the research has not been extensively studied as most research focuses on risks that prevent the product from reaching the final customer, not caused by the customer themselves. However customers do have an impact with the demands that they place on the focal firm (Neureuther and

Kenyon, 2009). The focus of the data review at the end of this paper will help examine how customer actions affect the supply chain disruptions.

Risk Identification

The supply chain is a large source of potential risk that has many opportunities for breakdown to occur. Supply chains have evolved to increase efficiency and reduce costs; the improvements being made to supply chains are very effective in normal operating conditions, making the supply chains flatter and requiring less coordination. However, this increased efficiency also makes the supply chain vulnerable to disruptions (Stecke and Kumar, 2009). Every organization looks at risk from a different perspective and there are many different classifications of risk. This paper will look at three different classifications of risk that range from broad to narrow, they can be used to identify where risk stems from and what characteristics it has.

The first categorization of was presented by Mitroff and Alpaslan (2003) the framework they presented is the broadest categorization of risk out of the three analyzed. The three broad categories they presented are natural accidents, normal accidents and abnormal accidents (Mitroff and Alpaslan, 2003). The first category of risks are natural accidents. This category of risk only has one subcategory which is natural disasters. Companies are prepared for the occurrence of a natural risk because they have experienced them in the past. They can prepare of these kinds of risk by doing safety planning and having insurance (Mitroff and Alpaslan, 2003).

Normal accidents are expected due to the complexity of technology, there should be expected system overloads and equipment malfunctions in any system. There are three

subcategories under normal accidents which are economic crises, physical crises, and personal crises. Mitroff and Alpaslan (2003) identify miscommunication as the main reason for normal risk. Some acts against a company are deliberate and calculated, such as product tampering or stealing, these acts are categorized as abnormal accidents. The three subcategories under abnormal acts are criminal crises, information crises and reputation crises. These types of risk are more prevalent today due to global terrorism and increased business in developing countries, yet are often the hardest for companies to imagine and plan for (Mitroff and Aplaslan, 2003).

Kliendorf and Saad (2004) categorizes risk into operational, natural hazards, terrorism and political risks. Operational risks stem from systematic failure in the supply chain. These can include equipment failing, abrupt discontinuity of supply and human created issues. Operational risks are the closest to the everyday operations of the supply chain. They have to deal with disruptions that happen in the supply chain at a particular company and halt the supply chain process. Examples of operational risks include, fires, equipment malfunction, accidents and strikes. Operational risks can also originate in the supply base and halt the production line in the focal firm. In 2004, General motors experienced one of the most prominent and effecting kind of operational risk, their workforce went on strike. In September 2004, 73,000 workers belonging to the United Auto Workers (UAW) union went on strike from their jobs (Isidore, 2007) Natural hazards are described as natural disasters that can create risk are hurricanes, storms, earthquakes and other natural issues that prevent businesses from operating correctly. A framework for reducing disaster risks in Supply Chains (2011) illustrates how detrimental

natural disasters can be on the supply chain. A study performed by Accenture concludes “...73% of executives saw disruptions in the supply chain in the last five years. Of those 36% say it took more than one month to recover” (Silva and Reddy, 2011). Natural Hazards include hurricanes, earthquakes and storms.

The third kind of distribution risk is terrorism, it can cause a major disruption in a supply chain, not only from the attack itself, but also from aftermath such as heightened security or clean up. Terrorism causes not only a threat to the security of a nation, but also threatens the efficiency and function of a supply chain. Political instability refers to circumstances or actions that affect the supply chain, including sabotage and destructive competitive acts. Political climate and policy can also pose a risk for the supply chain. Political risk can refer to the actual politics of a country where a supplier is located. Political policy that makes business harder to do will always be a risk that companies must overcome. Politically motivated actions also fall under political risk. For instance sabotage of a competitor or a supplier turning into a competitor by using a company’s own knowledge that they have acquired.


Chopra and Sodhi (2004) have created a more detailed framework for identifying potential risks to the supply chain. The categories they identified are disruptions, delays, systems, forecast, intellectual property, procurement, receivables, inventory, and capacity. The authors also identify what drives the risk in each of these categories. Disruptions are risks that disrupts that flow of material through the supply chain, including natural disasters, war or terrorism, supplier bankruptcy, single source dependency or labor disputes (Chopra and Sodhi, 2004). These disruptions can happen

internally or externally depending on where the cause of the disruption stems. The next category of risk are delays, which can be attributed to issues with the supply source. Issues that can arise are inflexibility, poor quality, and border crossing. Technology and communication are the main drivers of system disruptions. System disruptions occur when failures occur in the information infrastructure, system integration with suppliers or when companies are using e-commerce. Forecast risks are the result of improper inventory or demand forecasting. Drivers of forecasts risks can include long lead times, seasonality, product life cycles and the bullwhip effect.

Intellectual property risks can occur when the intellectual property of a company is not secure. Intellectual property can be put at risk when vertical integration occurs or when a company outsources globally; anytime intellectual property is shared outside of a company it has the opportunity to be compromised. Procurement risks has to do with the acquisition of supply. It is driven by exchange rate, raw material availability, industrywide demand, and contract length. Another risk category is receivables. This kind of risks stem from issues with the customer, including number of customers and the financial strength of the customer. Inventory risks have to do with the product itself. If the product has a high rate of obsolescence, high inventory holding costs, a high value, or demand and supply uncertainty; it becomes an inventory risk. Lastly, capacity risks include the cost of capacity and capacity flexibility. Capacity risks can happen externally or externally depending on where the issues occur in the supply chain. Table 1 summarizes all of the risk identification strategy examples explained above.

Table 1: Risk Identification Summary

	Author	Risk Identification Strategy
Broad ↑	Mitroff and Aplalan (2003)	Normal Accidents <ul style="list-style-type: none"> • Personal Crises • Physical Crises • Economic Crises
		Abnormal Accidents <ul style="list-style-type: none"> • Criminal Crises • Information Crises • Reputation Crises
		Natural Accidents <ul style="list-style-type: none"> • Natural Disasters
	Kliendorf and Saad (2004)	Operational Risks <ul style="list-style-type: none"> • Systematic Failures
		Natural Hazards <ul style="list-style-type: none"> • Natural Disasters
		Terrorism <ul style="list-style-type: none"> • Terrorist acts
		Political Risks <ul style="list-style-type: none"> • Corruption
	Chopra and Sodhi (2004)	Disruptions <ul style="list-style-type: none"> • Natural disaster • Labor dispute • Supplier bankruptcy
		Delays <ul style="list-style-type: none"> • High capacity utilization at supply source • Inflexibility or Supply Source • Poor quality or yield at supply source
		Systems

		<ul style="list-style-type: none"> • Information infrastructure • System integrate • E-Commerce
		Forecast <ul style="list-style-type: none"> • Inaccurate forecasts • “Bull-whip effect”
		Intellectual Property <ul style="list-style-type: none"> • Vertical integrate of supply chain • Global outsourcing risk
		Procurement <ul style="list-style-type: none"> • Exchange rate risk • Percentage of a key component or raw material • Industry wide capacity utilization • Long-term VS. short-term contracts
		Receivables <ul style="list-style-type: none"> • Number of customers • Financial strength
		Inventory <ul style="list-style-type: none"> • Rate of product obsolescence • Inventory holding cost • Product value
		Capacity <ul style="list-style-type: none"> • Cost of capacity • Capacity flexibility
	Narrow	

Disruption Severity

The severity of a supply chain disruption can range from company specific to globally impactful. Formally, the severity of a supply chain disruption can be defined as the number of entities (or nodes) within a supply network whose ability to ship and/or receive goods and materials has been hampered by an unplanned, unanticipated event” (Craighead, et. al., 2007, 134). Analysis of the severity a disruption can have on the supply network must begin with the analysis of how the supply chain is configured. A supply chain is made up of interconnected nodes or individual entities that are connected

by material flow. The interconnected nodes can also be referred to as the supply network and the focus company is the buying company that purchases from the supply network (Choi and Krause, 2006). The three areas that contribute to disruption severity and affect the flow of materials throughout this network are supply chain density, complexity and node criticality.

Supply chain density refers to how close or far apart the individual nodes of the supply chain are from their customer and from each other. The closer the nodes of the supply chain the more density is it said to have, while more distance between the nodes is said to have less density. (Craighead et. al., 2007). The complexity of the supply chain is how many elements contribute to the supply network. The complexity is further defined as the total number of nodes and the total number of forward and backward flow of the material within the nodes (Choi and Krause, 2006). Lastly, node criticality is how important a node is to the supply chain. All nodes in the supply chain should add value and contribute to the values stream for the focus company. Nodes can be deemed more or less critical depending on what kind of part they are supplying to the focus company (Craighead et. al., 2007). The nodes that are more critical will have a larger impact on the supply chain if they encounter a disruption Severity of disruptions can be due to a breakdown in any of these areas in the supply network.

Risk Mitigation

Risks need to be managed in order to keep them from spiraling out of control and to help companies stay productive in spite of disruptions. Companies can utilize many different strategies to help mitigate risk. The strategies that will be examined in this

section include proactive, reactive, abstract and specific strategies. Proactive strategies occur prior to an actual event happening, and often result from brainstorming potential risk areas, gathering support and training employees. Reactive strategies occur when an actual supply chain disruption is taking place. With reactive strategies it is important to identify the risk quickly and put a mitigation plan in place to overcome the disruption. Abstract strategies provide loose guidelines for companies to incorporate, but do not give a specific implementation plan. They are generally more long term goals and require a lot of coordination. Lastly, specific strategies focus on pinpointing risk areas and implementing very specific plans to help mitigate that one kind of risk. Most companies should use a combination of these different mitigation styles to help reduce the overall risk that the supply chain faces. The following strategies are examples of the different approaches a company could use in different risk situations.

The first risk mitigation strategy is laid out by Kleindorfer and Saad (2004). They propose a step by step process that allows companies to assess the vulnerability of their supply chain and proactively assign resources to the most critical parts of their process. The first step is to obtain senior management understanding and approval. The senior management has the ability to allocate financial resources to the project and sponsor necessary improvements. Without their approval, the strategy cannot move forward. Next, the company has to identify key processes that are likely to be affected by distribution. All processes and suppliers are not equal when it comes to risk susceptibility.

The critical areas of the supply chain need to be identified and addressed in sequential order from most critical to least. Resources should be allocated accordingly, beginning with the most critical processes first. Third, traditional risk management is undertaken for each key process to identify their vulnerabilities. The critical processes that were identified in step two are now analyzed individually for their vulnerabilities and create strategies that will help alleviate them if they occur. The last step is reporting, periodic auditing, management and legal reviews of plans for ongoing results. This step ensures that the strategies comply with legal standards and management policy. It also has a review component that ensures that strategies are up to date and are being applied to the most critical part of the supply chain. If any changes occur the process should be repeated and continuously checked (Kleindorfer and Saad, 2004).

Another way to look at risk mitigation is by improving the information that supply chain managers receive. Christopher and Lee (2004) propose a mitigation strategy centered on improving confidence in the supply chain. This is an example of an abstract strategy that pinpoints drivers that help mitigate risk, however it is up to each individual firm to deploy a strategy to implement them. They suggest that visibility and control are two major factors that modern supply chains are lacking. Visibility refers to the insight that a company has into their supply chain operations. With the increase in globalization it is often hard to have insight into the end-to-end pipeline of the supply chain (Christopher and Lee, 2004). Increasing visibility should be a major goal of the company to mitigate risk. Having more open communications with channel members is an important way to increase visibility. "...information-enriched supply chains perform significantly better

than those that do not have access to information beyond their corporate boundaries” (Christopher and Lee, 2004).

Improved confidence is also affected by the amount of control that a firm has over supply chain operations. Even when a manager has visibility into the operations of their channel members they may not have the control to make changes in the short term (Christopher and Lee, 2004). Creating a more responsive supply network would allow companies to control decisions more readily, thus giving them more confidence about the decisions they are making. Enhancing visibility and control of the supply chain will mitigate risks by increasing the confidence that managers have in their decisions making and will create a more responsive system when risks do occur.

Chopra and Sodhi (2004) provide a multitude of specific risk mitigation strategies for companies to explore based on their chance of risk and the cost of implementing a risk management strategy. The interconnected nature of supply chain risk makes risk mitigation a hard task, because actions that mitigate one risk may exacerbate another (Chopra and Sodhi, 2004). Their strategy advocates holding reserves that will help mitigate risks when they should occur. They should focus on placement, size and cost of the reserves, without decreasing profits (Chopra and Sodhi, 2004). The reserves that a company should focus on are excess inventory, excess capacity and redundant suppliers. The strategies that can utilize these reserves are increase capacity, acquire redundant suppliers, increase responsiveness, increase inventory, increase flexibility, pool or aggregate demand, and increase capacity (Chopra and Sodhi, 2004).

Each of these strategies helps mitigate a different risk in the supply chain. After a company identifies their most pressing risks, they can then implement these strategies; keeping in mind that some other risks might be magnified when they choose one mitigations strategy. To help a company choose, managers should perform stress testing and tailoring. Stress testing is a way for managers to answer “what-if” questions and focus on the critical parts of their supply chain (Chopra and Sodhi, 2004). Stress testing identifies key parts of the supply chain and probing for potential sources of risk, helps a company identify where to focus their reserves. After stress testing is completed, the company can then tailor their approach to mitigate the risk. Tailoring has three relationships to consider; increasing cost of risk reduction, pooling forecast risk, and benefit of pooling grows with level of risk (Chopra and Sodhi, 2004). Managers should balance these risks when finding a strategy for their supply chains.

The last kind of framework presents a reactive mitigation strategy that helps a company recover after a risk has impacted the supply chain. The goal of this kind of strategy is to get a supply chain back in working order as quickly as possible. Macdonald and Corsi (2013) look at the overall disruption management process, providing analysis of how to manage and recover from a supply chain disruption. They identify discovery, recovery and redesign as the three stages of post event disruption management (Macdonald and Corsi, 2013). The key phases are the discovery and recovery phases as they are the most immediate steps that need to be addressed.

The first phase is the discovery phase, “discovery refers to the point in time when people become aware of the event of supply chain disruption” (Macdonald and Corsi,

2013, 272). This is a critical stage as managers must react quickly to assess the severity of the situation. Managers, in this step previous risk planning will come into play, as managers can use any previous plans or experience to mitigate the current risk. After the prior planning has been reviewed managers need to start the recovery process. Recovery is the next stage in the reactive method, when action is taken to mitigate the supply chain risk (Macdonald and Corsi, 2013).

There are two elements that make up the recovery process, structural and behavioral. The structural element is centered on the decision making structure. Designating one primary decision maker to lead the recovery effort is often helpful to help streamline the recovery process (Macdonald and Corsi, 2013). Behavior refers to the attributes of the people involved, including if they follow contingency plans, employee training, and time sensitivity (Macdonald and Corsi, 2013). Lastly, the company needs to learn from their experience and redesign their processes to help mitigate future risk. It is important to update the contingency plans, to help make the discovery and recovery phases of subsequent risks shorter and less impactful.

Macdonald and Corsi (2013) suggest that proper disruption management will lessen the overall impact that a supply chain disruption has on the overall performance of the supply chain. Service and financial impact are the two main factors that can be lessened through correct disruption management. Service failures occur because the company does not devote as much attention to their other processes while trying to recover from the disruption (Macdonald and Corsi, 2013). Financial impact refers to the cost incurred as a result of the disruption. These two factors can affect a company's

reputation and bottom line, therefore the disruption management process is designed to help mitigate these issues and return the supply chain to working order.

CUSTOMER FACING RISK DRIVERS

A supply chain faces vulnerability points at the supplier, firm and customer level. Most of the research surrounding supply chain risk focuses on the supplier and firm, however little research has been done looking at how a customer can affect a supply chain and potentially put it at risk. This paper will strive to close this gap by demonstrating how a customer can place the supply chain at risk, by looking at factors that the customer affects, analyzing out of stock data from a consumer packaged goods manufacturer as well as making some recommendations on how to mitigate customer risk.

The Customer's operations, decisions, and profitability can have a major effect on the focal firm's supply chain. First, the operations of a customer can greatly affect supply chain risk, through their forecasting. Firms rely on demand forecasts to determine how much product will be needed. If a customer over forecasts demand they will have excess product that is not sold. This means that the focal firm has sent product to their customer that they did not need, however another customer in their supply chain might have utilized. On the other hand, the customer may under forecast, leaving them with a stock out. This is also an issue because the manufactures brand is no longer in that store and they may lose business to competitors.

Customers also affect supply chain risk through their decision making. The customer has the power to make demands, choose what merchandise to place in their

store, location in the store and the amount of merchandise they will carry. Because of this power, the customer can place demands on the focal firm to deliver the products they want. The customer can also place demands to rush orders or expedite shipments that may also strain supply chain operations. Lastly, the customer is the source of revenue to the focal firm. Timely, accurate and dependable payments are important to the focal firm to continue their operations and pay their own suppliers in a timely fashion. This dependent relationship can cause risk to increase if customers withholds payment from the focal firm, without funding the supply chain can suffer.

Data Analytics

For the consumer packaged goods manufacturer whose data was used for this study, I analyzed how existing metrics that they are already tracking will help identify where customers contribute to supply chain risk. First, let's examine the structure of the customer facing supply chain. This particular manufacturer has a two-tier distribution system where they utilize distributors to get their product out to the end customer. The manufacturer breaks the country into 5 regions Central, Great Lakes Northeast, Pacific, and Southeast. This company defines out of stock as any instance when the product is not available in the retailer. They track individual instances of product stock out, meaning that each individual SKU is tracked and every stock out is reported. Utilizing the existing raw data, of stock out codes, I assessed the risk that the customers place on this particular commercial manufacturer.

The data this manufacturer receives, comes in a weekly report that has out of stock codes for every retailer that sells their product across the United States. To make

the data meaningful it had to be cleaned, and analyzed to provide information to the company that will allow them to assess customer risk. This weekly data was first compiled into monthly segments to track out of stock data for each individual month. Then, the data was broken out into each region that the company services. The out of stock codes were grouped by out of stock codes for each month and then aggregated for six months of data. Exhibit 1, displays the breakout of the out of stock codes by region.

Six months of stock out data was sorted by out of stock code for each region where the company operates. Exhibit 1, shows the breakdown of all the out of stock codes for the regions based on the individual instances. Although this data shows the break out of where the codes occur, they are not meaningful to managers because they are not grouped by similarities nor can they assign resources to all of these individual codes. To help make these codes meaningful the Chopra and Sodhi (2004) framework will help categorize these into meaningful segments that can be managed.

Exhibit 1: Out of Stock Codes by region

	Central Region	Great Lakes Region	Northeast Region	Pacific Region	Southeast Region	Grand Total
Did not meet minimum run requirements	49	28	26	-	21	118
Didn't order to target	2,042	3,296	1,118	1,125	2,561	9,794
In Transit	61	473	332	189	438	1,402
Other-Please explain	521	73	211	31	68	895
Over sold forecast	1,505	2,194	932	1,508	664	6,440
Product cut from order	278	566	222	188	146	1,374
Rarely orders	535	828	481	213	316	2,309
Rarely orders/very low	44	157	32	77	40	344

volume (POINT ONLY)						
Shipment delay	613	1,347	853	459	1,011	3,981
Transportation Issues	65	86	58	24	117	350
Grand Total:	5,713	9,048	4,265	3,814	5,382	27,007

Applied Framework

The Chopra and Sodhi framework will be utilized because it has the most narrow risk identification method that will allow this manufacture to pinpoint specific ways that they can mitigate the most prominent customer driven risks. The seven areas of risk that were identified are capacity, forecast, disruption, inventory, procurement delays and other. The company's out of stock codes were mapped to Chopra and Sodhi's framework in order to classify the types of risk that impact the supply chain. The breakdown of the out of stock codes is depicted in Table 2. From these classifications, managers will be able to accurately assess what kind of risk the out of stock codes create, which are the most pressing, and where to deploy resources.

Table 2: Categorized Out of Stock Codes

Risk Identifier	Out of stock code
Capacity	Did not meet minimum run requirements
Forecast	Didn't order to target Oversold forecast
Disruption	In- transit
Inventory	Product cut from order
Procurement	Rarely orders Rarely orders/very low volume
Delays	Shipment delays Transportation issues
Other	Other

Results

After the company classifies their out of stock codes and separates the risks by region, they can focus on their most risky areas. According to Exhibit 3, the most risky regions that this commercial product manufacturer has are the Great Lakes Region and the Central Region. These areas have the greatest total risk factors. Exhibit 4, shows the areas of risk that have the most overall effect from the customers across all of the regions. Utilizing both of these categorizations, this manufacture can see where supply chain risk has the most potential to occur and monitor these risky areas.

Exhibit 3: Customer Facing Risk Breakdown by Region

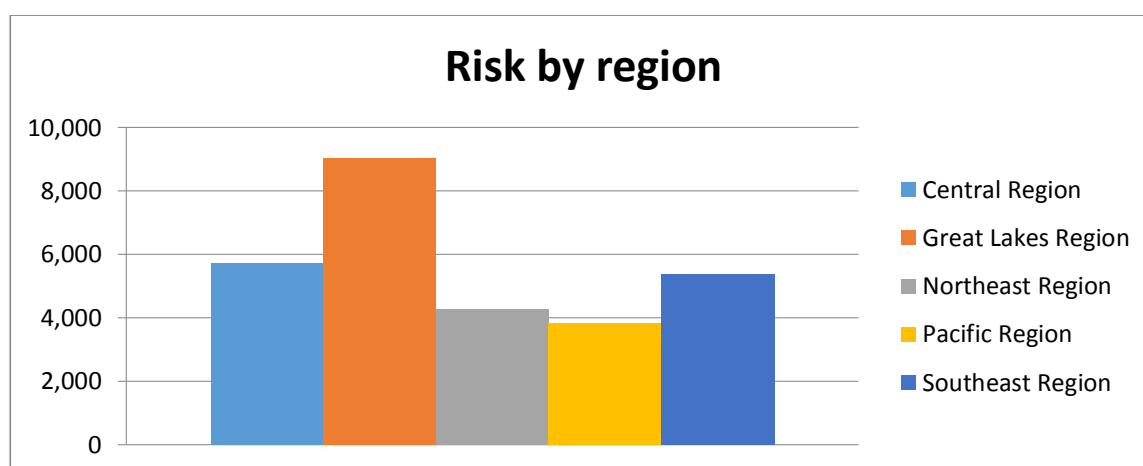
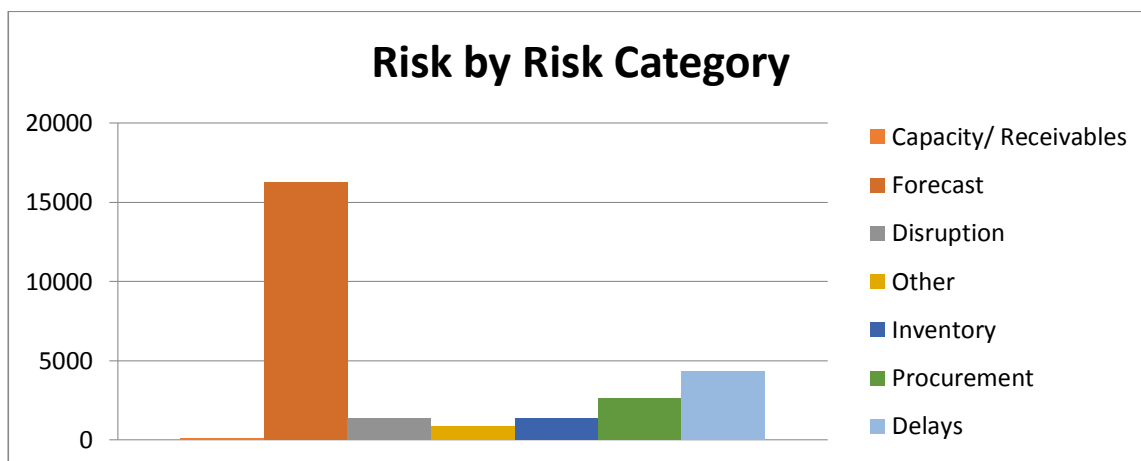


Exhibit 4: Customer Facing Risk Breakdown by Risk Category



CONCLUSION

Supply chains are becoming inherently more risky. According to a survey conducted in 2013, more than eight out of ten were affected by a supply chain disruption during the past two years (Mohamed, 2013). As the modern supply chain grows and develops, it is actually becoming less flexible and autonomous. The result is that supply chain risks will have a bigger impact. This larger risk, only creates a stronger need for identification and mitigation strategies to be in place and actively used. Preparation for these events can mean the difference between recovery and financial ruin.

All supply chains will face risks, strains and disruptions; the important factors are identifying the critical areas where these risk occur and prioritizing the most hazardous risks. Companies must not only have the foresight to identify risk, but also to realize that they cannot stop them from happening. Instead, companies need to be asking “what-if” questions that will help determine what a supply chain disruption will cause (Field, 2013). Looking at the implications of losing a key supplier or not having enough capacity will help managers take action to figure out what the plan will be after a risk occurs.

Managers also need to prepare for the financial implications that occur in conjunction with a supply chain disruption.

Companies are lacking a risk culture that is able to effectively recognize an escalating risk and take appropriate measures to mitigate these risks (Field, 2013). By putting different identification and mitigation strategies into place, managers can focus their resources and create a supply chain that is better prepared to handle risk. Also recognizing the supply chain as an interconnected entity and knowing that risk can occur throughout the entire process will, also create informed managers who can better prepare for the risky future that lies ahead.

REFERENCES

- Aven, T., & Renn, O. (2009). On risk defined as an event where the outcome is uncertain. *Journal of Risk Research*, *12*(1), 1-11.
doi:10.1080/13669870802488883
- Choi, T. Y., & Krause, D. R. (2005). The supply base and its complexity: Implications for transaction costs, risks, responsiveness, and innovation. *Journal of Operations Management*, *24*, 637-652. doi:10.1016/j.jom.2005.07.002
- Chopra, S., & Sodhi, M. S. (2004). Managing risk to avoid supply-chain breakdown. *Sloan Management Review*, *46*(1), 53-61.
- Christopher, M., & Lee, H. (2004). Mitigating supply chain risk through improved confidence. *International Journal of Physical Distribution and Logistics movement*, *34*(5), 388-396. doi:10.1108/09600030410545436
- Craighead, C. W., Blackhurst, J., Rungtusanatham, M. J., & Handfield, R. B. (2007). The severity of supply chain disruptions: Design characteristics and mitigation capabilities. *Decision Sciences*, *38*(1), 131-156. doi:10.1111/j.1540-5915.2007.00151.x
- Field, A. M. (2013, February 4). Preparing for the worst: developing a more structured, strategic approach to supply chain risk mitigation. *Canadian Sailings*, 11-15. Retrieved from http://greatwhitepublications.ca/Issues/weekly/feb_13/feb_4_2013.pdf
- Isidore, C. (2007, September 24). 73,000 workers walk in nationwide GM strike. *CNN money*.

- Kleindorfer, P. R., & Saad, G. H. (2005). Managing disruption risks in supply chains. *Production and Operations Management, 14*(1), 53-68. doi:10.1111/j.1937-5956.2005.tb00009.x
- Macdonald, J. R., & Corsi, T. M. (2013). Supply chain disruption management: Severe events, recovery and performance. *Journal of Business Logistics, 34*(4), 270-288.
- Mitroff, Ian I, & Alpaslan, Murat C (2003). *Preparing for Evil* (RO304J). Boston?: Harvard Business School Pub.
- Mohamed, M. (2013). How to Reduce and Recognize Risk. *CSCMP's Supply Chain Quarterly, 7*(3), 32-37.
- Nelson, D., Mayo, R., & Moody, P. E. (1998). Powered by Honda: Developing Excellence in the Global Enterprise.
- Neureuther, B. D., & Kenyon, G. (2009). Mitigating Supply Chain Vulnerability. *Journal of Marketing Channels, 16*, 245-263.
doi:10.1080/10466690902934532
- Rice, J., & Caniato, F. (2003). Building a Secure and Resilient Supply Chain. *Supply Chain Management Review, 7*(5), 22-30.
- Silvia, J., & Reddy, S. (2011). A Framework for Reducing Disaster Risks in Supply Chains. *International Journal of Business Research, 11*(4), 112-117.
- Simpson, L. (2002). Docks battle makes worldwide waves. *Supply Management, 7*(23), 26-8.

- Stecke, K. E., & Kumar, S. (2009). Sources of supply chain disruptions, factors that breed vulnerability, and mitigating strategies. *Journal of Marketing Channels*, *16*, 193-226. doi:10.1080/10466690902932551
- Wagner, S. M., & Neshat, N. (2012). A comparison of supply chain vulnerability indices for different categories of firms. *International Journal of Production Research*, *50*(11), 2877-2891. doi:10.1080/00207543.2011.561