Research Project

on

Supply chain risk in computer industry

Bachelors of Business Administration

(Logistics & SCM)

(Established under Galgotias University Uttar Pradesh Act No. 14 of 2011)

Under the guidance of: Ashok Kumar Sharma

Submitted by: Kajal Shivhere

BBA 6th sem

(Logistics & SCM)

18SLAM1010001

Certificate

This is to certify that Kajal Shivhare (18SLAM1010015), final year student of BBA Logistics and supply chain management of Galgotias University has made his SIP report on the topic “Supply chain risk of computer Industry” under the guidance of Prof. Ashok Kumar Sharma (H.O.D Logistics and supply chain management) in October 2020.

Singature:

Declaration

hereby declare that the work done on the SIP report made on the topic of “Supply chain Risk of computer industry”is solely done by me. No part of it is taken from any other source and is my original work.

Kajal Shivhare

Acknowledgement

I would like to express my special thanks of gratitude to Prof. Ashok Kumar Sharma as well as Prof. Avdhesh Kumar Yadav who gave me the golden opportunity to do this wonderful project on the topic “Factor affecting LSCM” which also helped me growing my knowledge and I came to know about so many new things.

I am really thankful to them.

Secondly I would also like to thank my parents and friends who helped me a lot in finishing this project within the limited time.

Thanks again to all who helped me.

Kajal Shivhare

Abstract

The purpose of this project is to go through the different research paper who had worked on the last mile design. Since it is one of the major part of the supply chain that needs to be worked on, it is very crucial to know the ways to reduce the cost and increase the customer satisfaction. The major sector where this plays a very important role is the e commerce. In this we will talk about the different variable that affect the last mile of the logistics.

Introduction

Cyber security is generally thought of as various types of security devices like firewalls, Web Application Firewall (WAF), IDS/IPS, SIEM, DLP etc. to safeguard network, applications and data. But what if, for example, the deployed security solutions have a bug inside? The latest example of this is exposing of a vulnerability in Lenovo notebooks. Lenovo notebooks are shipped with a program named “Superfish-Visual Discovery”, and recently a vulnerability known as Man-in-the-Middle (MITM) has been discovered in this software, so all the security controls installed in the notebooks like antivirus etc. cannot catch it, because it is the default shipped in the software. This is an example as to how important is to take not only networks but also each component of a supply chain into consideration.

Cyber security in the supply chain is a subset of supply chain security and is focused on the management of cyber security requirements for information technology systems, software and networks, which are driven by threats such as cyber-terrorism, malware, data theft and the Advanced Persistent Threat (APT). Typical supply chain cyber security activities for minimizing risks include buying only from trusted vendors, disconnecting critical machines from outside networks, and educating users on the threats and protective measures they can take.

information and communication technology (ICT) is exponentially growing in Supply Chain Management (SCM) for increasing productivity and profitability in business. This growth of Information Technology in SCM has changed the paper based environment to Virtual Supply Chain, which is also generating electronic risks (e-risks) in form of cybercrime or fraud. Although, reducing the e-risks from huge data generated in day to day operation of supply chain networks is a big challenge for decision makers, auditors, detecting and investigating agencies.

We know that technology is always a double-edged sword which can be reciprocally used for prevention of e- risks in SCM. The purpose of these empirical studies is to discuss the IT application and trend to curb the supply chain’s e-risks. Key words: e-risk, information technology (IT), supply chain management (SCM).

The U.S. computer industry is seen as "saturated," Lane said. "With the emergence of cell phones and with increased computing and Internet capabilities, there has been a notable slowdown in the sales of personal computers to consumers."

However, he said two industry trends will help computer manufacturers experience continued growth in 2007: the shift in preference to notebooks and laptops, and the arrival of new computers on the market designed to carry the new Microsoft Vista operating system.

The price war to attract consumers will most likely continue -- and possibly worsen conditions for suppliers -- as the U.S. economy continues to experience a slowdown. North said that businesses that rely on consumer spending may see tougher times ahead as housing market equity, which has fueled consumer spending in the past, continues to fall .

"The battle between computer manufacturers to provide more efficient and less expensive systems has been a beneficial trend for consumers, but a hurtful development for the companies that are providing the materials to manufacture the machines,

Description

To successfully control costs, manage risk, and scale operations, logistics leaders must have visibility into every element of their operations. But, with different teams using various systems, applications, and documents to manage workflows, achieving this end-to-end transparency can be nearly impossible.

But it doesn't have to be.

The "secret sauce" of taking your logistics to the next level is through the implementation of a low-code platform. Low-code is a modern, agile way to build and continually improve business software applications, to better match the pace of change in today's digital business environment.

Join us October 15th to uncover How to Achieve End-to-End Visibility in Logistics. Our speakers will walk through how large-scale global organizations are achieving real-time visibility across their supply chains.

By leveraging a low-code platform, logistics leaders across industries have been able to connect disparate sources of data and information – from ERPs to one-off spreadsheets – and achieve real-time visibility across departments, locations, and teams. Join us to learn how you can do the same, including.

Cyber Security Threats in Supply Chain

The below section will show some examples of cyber security threats in the supply chain:

- Network or computer hardware that is delivered with malware installed on it already (such as Superfish installed on Lenovo notebooks).
- Malware that is inserted into software or hardware (used by Dragonfly cyber group, discussed later in the document).
- Vulnerabilities in software applications and networks within the supply chain that are discovered by malicious hackers.

Cyber Security Scope in Supply Chain

Cyber security of any one organization within the chain is potentially only as strong as that of the weakest member of the supply chain. A determined aggressor, notably advanced persistent threats (APTs), will make use of this by identifying the organization with the weakest cyber security within the supply chain, and using these vulnerabilities present in their systems to gain access to other members of the supply chain. Whilst not always the case, it is often the smaller organizations within a supply chain who, due to more limited resources, have the weakest cyber security arrangements.

Cyber security is needed in all phases of a particular supply chain because an organization cannot be sure from where a risk will evolve. One example I have already given is regarding the vulnerability in the packaged software in Lenovo notebooks. Another example will be of a particular code behind a software. Areas of concern for an organization will be like who all has access to code? Who has written the code? Where it is stored? How can tampering in the code be detected?

So cyber security fits in all phases of a particular supply chain, whether it is a hardware supply chain or a software supply chain, though a software supply chain is more important.

Compliance Requirements for Cyber Security

Various compliance regulations such as PCI DSS clearly articulate in their requirements about how to manage risks in the supply chain, whether that includes an internal process or involvement of third party service providers, merchants etc.

For example, PCI DSS 3.0 includes requirements like penetration testing, application development lifecycle security, and threat modeling – all facts to the point that supply chain risks are an escalating concern. PCI DSS 3.0 requirements indicate that a downstream software supply chain is an emerging attack vector.

It is very important for organizations to understand that to cover cyber risks in a supply chain, organizations not only need to assess everything in their internal environment but also for all the actors involved in the supply chain.

For example, credit card organizations which are compliant with PCI DSS need to assess risks with merchants, distributors, credit card makers, banks, service providers – i.e., all the actors involved in the complete supply chain.

Cyber Security Outbreak: Recent Examples in Supply Chain

This section will illustrate the recent examples that have led to greater emphasis on covering cyber security risks in the supply chain.

1. A recent example of this is the installation of adware known “Superfish” in Lenovo notebooks. End users cannot detect it to be malicious nor will the antivirus software installed on the system, because software of this kind needs to be trusted since they come by default. Superfish software tends to install a self-signed root HTTPS certificate that can intercept encrypted traffic for every website a user visits. When a user visits an HTTPS site, the site certificate is signed and controlled by Superfish and falsely represents itself as the official website certificate.

2. Even worse, the private encryption key accompanying the Superfish-signed Transport Layer Security certificate appears to be the same for every Lenovo machine. Attackers may be able to use the key to certify imposter HTTPS websites that masquerade as Bank of America or any other secure destination on the Internet. Under such a scenario, PCs that have the Superfish root certificate installed will fail to flag the sites as forgeries—a failure that completely undermines the reason HTTPS protections exist in the first place.

3. A cyber espionage group named Dragonfly was able to attack the pharmaceutical sector by setting up trojans in legitimate software. Because of this plantation of trojans in the supply chain, the Dragonfly group was able to control the now malicious software by replacing legitimate files with malicious files in the software. This malicious software in result, when downloaded from the supplier’s website, provided remote access functionalities that could be used to take complete control over the system where the software was installed, or it could have been used to make the remote system act like a bot.

1. Another example of cyber attack risks in the supply chain is that of shylock banking trojans. Attackers use the website builders to compromise legitimate web sites by redirecting their requests to a malicious domain. As soon the request lands onto the malicious domain, malware gets downloaded onto the system and thus attacks like man in the browser was performed. This attack is so severe that it even avoids detection and protects itself from analysis. Thus attackers target the website builder used by many companies, thereby infecting at a large magnitude.

2. Another great deal of cyber risks involved in a supply chain is involvement of third parties, which are often used to store confidential data. Similarly, an attack was observed on large data aggregators where a small botnet was transferring data from the internal systems to a botnet controller on the Internet through the encrypted channel. This attack has resulted in theft of a data aggregator that licenses information to use in credit decisions

Key Practices in Cyber SCRM

The *NIST Framework for Improving Critical Infrastructure Cybersecurity* ("the Framework") released in February 2014 was published simultaneously with the companion *Roadmap for Improving Critical Infrastructure Cybersecurity*. The Roadmap identified Cyber Supply Chain Risk Management (Cyber SCRM) as an area for future focus. Since the release of the Framework and in support of the companion Roadmap, NIST has researched industry best practices in cyber supply chain risk management through engagement with industry leaders.

In 2014 and 2015, NIST interviewed a diverse set of organizations and developed 18 Cyber SCRM Case Studies describing how various industry organizations approach Cyber SCRM, including specific tools, techniques, and processes.

In 2019, NIST conducted new research aimed at identifying how Cyber SCRM practices have evolved. For this newest set of Cyber SCRM Case Studies, NIST conducted interviews with 16 subject matter experts across a diverse set of six companies in separate industries. These interviews informed a Summary of Findings and Recommendations document describing trends, correlations, and novel findings garnered from an analysis of the interviews as a whole.

NIST has used the SCRM Case Studies published in 2015 and 2019, prior NIST initiatives, and a number of standards and industry best practices as a basis for NISTIR 8276, *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry*

Risks and their management in supply chains

The particular and complex characteristics of supply chains require tailor-made risk management actions, given that the unit of analysis is a business relationship among several companies that are susceptible to different risks
Risk has a huge range of definitions depending on the field of research. These can be found in the literature on risk in the areas of finance, marketing, management and psychology among others Another characteristic presented by these and other authors, such as is that a constant dichotomy exists between a purely negative risk and one that can also provide an opportunity.

Specifically in supply chains, risk is generally perceived for its undesirable consequences, so that its negative character prompts the need for its management and employ a specific concept for risk in supply chains, according to which it is the potential occurrence of an incident, associated with failings of suppliers that can result in the inability to meet demand correctly and/or safely.

It is possible to identify in the literature business trends and other reasons able to make the chain more vulnerable, such as opportunities to compete globally, increasing the exposure of the chain and adding new risk dimensions. According to , firms are forced by current trends to think about global markets, both regarding customers and suppliers. While internationalization provides opportunities to increase revenues and lower costs, it also raises the complexity of supply chains, and hence their vulnerability to risks and the difficulty of managing them.

The risk management is a process where decisions are made to accept, avoid, transfer or share a known risk, or also to implement actions to reduce the consequences or probability of occurrence of an adverse event.

In particular, according to , supply chain risk management (SCRM) is an offshoot of supply chain management whose study has been gradually attracting more attention, to analyze the theoretical imperatives and practical needs to mitigate the risks to which supply chains are subject.

Some aspects that increase interest in the subject are mentioned by , among them strategies and structures related to chains, which are growing quickly and evolving in the effort to find competitive advantages.

Factors that generate supply chain risks and their classification

Opportunities to compete globally increase the exposure of chains and add new risk dimensions state that firms are forced by current trends to think globally, both in terms of customers and suppliers point out some of the advantages of globalization to supply chains, such as access to new sources of raw materials and more specialized and/or cheaper labor and better installations for production and distribution in strategic markets. However, despite the opportunities for higher revenues and lower costs, internationalization increases the complexity of chains, and hence the vulnerability to risks, making them harder to manage affirm that while global operations substantially reduce costs, they also make supply chains more vulnerable to risks.

Increasing interdependence of members: Solid partnerships are important positive factors for companies, by reducing transaction costs, allowing firms to concentrate on their core activities and facilitating access to technology and information. However, this interdependence can also pose risks, such as resistance to change, disagreement over practices among the members and relationship conflicts. Moreover, there is a much greater need for efficient and reliable information and production systems, in their study of supply chain risk management during periods of financial crisis, detected evidence of a higher number of bankruptcies in 2008 and 2009 (financial crisis in the USA) compared to previous years, suggesting a chain reaction, explained as the consequence of increasing interdependence.

Outsourcing: According to , outsourcing has become a very effective strategy for firms to focus on their core business. Among the advantages are reduction of labor costs and more specialized attention by outside parties to non-core activities and explain that outsourcing makes companies increasingly interdependent and the respective supply chains harder to control. The occurrence of accidents and other risks affecting suppliers can cause large losses. For example, in 2001 Land Rover had to spend millions of dollars to prevent the shutdown of production and loss of 1,500 jobs due to the bankruptcy of a supplier.

Strategies like Lean Six Sigma and Just in Time: According to and these methods are efficient and implementing them has become a factor of status of companies, often seen as the only way to remain competitive. However, the authors point out that this makes supply chains more vulnerable, because, as also noted by , the reserve stocks of input materials and/or finished products can be insufficient in case of a disruption in the chain, jeopardizing revenues, image and trust of customers.

Reduction of the base of suppliers: and highlight the risks of this strategy to business continuity, since firms should not only be concerned with risks related to their own continuity, but rather that of the entire chain. Another risk related to reducing the base of suppliers is the lead time required by each of them. According to companies face substantial increases in risks of shutting down production lines, and thus reducing their return on investments, when they have a single supplier and there are changes in its lead time.

Chart 1 Classification of supply chain risks.

Authors	Classification
(Pfohl et al., 2011)	Internal risks of the company, external risks inside the supply chain, and risks outside the chain.
(Singhal et al., 2011)	Risks with operational, market, strategic, product or mixed characteristics.
(Khan & Burnes, 2007)	Technological or strategic risks.
(Wagner & Bode, 2008)	Risks of demand; supply; regulatory, legal or bureaucratic; infrastructure; and catastrophes.
(Ghadge et al., 2012)	Organizational risks; inventory risks; process or operational risks; quality risks; network, relationship risks; environmental risks.
(Rangel et al., 2014)	Development of 20 risk classifications, and identification of 56 types of risks within the classifications, to support the process of possible mitigation. The categories are: production flow, relationships, competitiveness, global problems, main competency problems, lack of control of the external environment, regulatory and legal, financial market, financial capacity, demand forecast, logistic problems, transport within the chain, information system problems, cultural differences, strategic, production capacity, infrastructure, service level, organizational, and other problems.

METHODOLOGICAL PROCEDURES

1 Classification of the study

This study can be classified as having a qualitative approach, because according to in this type of study the researchers are subjects and objects at the same time, and the objective is to produce in-depth and illustrative information from a sample, whether large or small. And according to, qualitative research involves examination of the universe of meanings, motives and attitudes, in line with the design of this study.

It is also an applied study, because it generates knowledge for practical application, aimed at solving specific problems. With respect to objectives, it can be considered an exploratory study, which generally involves literature review, interview with people to elicit their practical experiences and analysis of examples to facilitate .

According to the technical procedures employed, this is a case study. According to , a case study is a type of history of a phenomenon, extracted from sources of evidence where any relevant fact to the events is a target of analysis. The procedures are described next.

2 Procedures

Step 1: Literature Review – We conducted a bibliographical search for relevant articles using the Web of Science™ database, filtered by topic (considering the title, abstract and keywords): "Supply Chain Risk Management", and also filtered by article type and by language (English and Portuguese). Of the 145 articles found, we read 130.

Step 2: Case Study – We formulated a structured questionnaire considering the risk taxonomy presented in Chart 2. This taxonomy was prepared based on the literature covering SCRM and the questionnaire was applied in an automotive company.

Chart 2 Risk taxonomy used in the study.

Risks	Description	Authors
Supply	Based on disturbances in the flow between the firm and supplier, any risk that keeps the supplier from delivering inputs reliably.	Diabat et al. (2012), Pfohl et al. (2010), Scannell et al. (2013).
Environmental	Risks that are outside the supply chain, such as economic crises, strikes and normative changes.	Pfohl et al. (2010), Jüttner (2005).
Demand	Risks associated with mismatch between the availability of final products and demand from customers, including excess stocks, mistaken introduction of new products, variations in demand, etc.	Ghadge et al. (2012), Diabat et al. (2012), Mentzer &Manuj (2008).
Discrete	Among the risks exogenous to the chain are discrete events, generally unforeseeable and with large negative impacts, such as terrorist attacks, contagious disease outbreaks and natural disasters.	Trkman& McCormack (2009).
Operational	These risks are related to technical failures, losses during the production process, alterations in production and technological changes, etc.	Diabat et al. (2012), Tang (2006), Shi (2004).
Rupture	These risks are associated with disruptions caused by natural catastrophes and human actions, such as terrorist attacks, earthquakes, floods, hurricanes, etc. They can be caused by a single factor or a set of factors.	Tang (2006), Shu et al. (2014).

Step 3: Data Treatment – To analyze the ranking of the criteria, we used the analytic hierarchy process (AHP), developed by Saaty, which is a multi-criteria method to support decision-making.

According to, the AHP is widely used by companies to address problems involving relevant decisions.

1. Representation of the hierarchy: development of the decision-making hierarchy associated with the various related levels;

2. Comparison of pairs: analysis of preferences related to each decision element of each hierarchical level;

3. Eigenvalue calculation: estimation of the relative weights of the decision elements of each hierarchical level and evaluation of the consistency of the pairwise comparison;

4. Aggregation of priorities: aggregation of the relative priorities to assess the result obtained in relation to the objective.

Chart 3 Fundamental scale of Saaty.

1	Equal importance	Two activities contribute equally to the objective
3	Weak importance of one over another	Experience and judgment slightly favor one activity over another
5	Essential or strong importance	Experience and judgment strongly favor one activity over another
7	Very strong or demonstrated importance	An activity is strongly favored and its dominance is demonstrated in practice.
9	Absolute importance	The evidence favors one activity over another The results of the survey indicated the factors considered by the respondent to have the highest priority in each category, as can be observed in the boxes in Figure 1. For example, delivery delay had a priority of 0.6 while failure to deliver
2, 4, 6, 8	Intermediate values between two adjacent judgments	When compromise is needed between two definitions

CONCLUSION

The results of the survey indicated the factors considered by the respondent to have the highest priority in each category, as can be observed in the boxes in . For example, delivery delay had a priority of 0.6 while failure to deliver material had a priority of 0.5.

In general, the objective of the study was achieved, of ranking the risk factors by applying the AHP. It is a technique to support decisions, and the results can serve to help not only the company studied, but other researchers and practitioners, who can use it to prioritize risk factors. Considering the attributes of risk (frequency and gravity), it is possible to establish a work flow in companies to analyze and measure risks.

The literature on SCRM describes the steps for risk management, namely identification, evaluation, mitigation and control. In line with these steps, to conduct an AHP it is first necessary to identify the risk factors. This can be done through brainstorming or by consulting historical data on the company's operations. Each area of the firm should be heard to identify these factors.

Next, evaluation is necessary, as presented in the theoretical framework, to prioritize the criteria/sub-criteria by comparing the probabilities and consequences. The questionnaire used in the interview indicates the attributes of the risk factors, to enable their evaluation.

This is the step of risk management where the AHP contributes the most. Based on the identification of the risk factors and their attributes, a method is necessary to evaluate them. This can be done subjectively, based on the experience and gut feeling of the professionals involved, but this can lead to a biased assessment.

BIBLIOGRAPHY

1. https://medium.com/@KodiakRating/the-cyber-security-of-supply-chains-whos-the-real-risk-man-or-machine-ecdcc365d49d#:~:text=Poor%20information%20security%20practices%20by%20lower%2Dtier%20suppliers.&text=Compromised%20software%20or%20hardware%20purchased%20from%20suppliers.&text=Software%20security%20vulnerabilities%20in%20supply%

20chain%20management%20or%20supplier%20systems.&text=Counterfeit%20hardware%20or%20hardware%20with%20embedded%20malware.

2. https://digitalguardian.com/blog/supply-chain-cybersecurity

3. https://heimdalsecurity.com/blog/supply-chain-cyber-security/

THANK YOU