Supply Chain Related Cyber Attacks

Gaurav Ghosh and Pawan Bhandari
Department of Automotive and Manufacturing Engineering Technology
Minnesota State University Mankato,
MN 56001, USA
gaurav.ghosh@mnsu.edu
pawan.bhandari.2@mnsu.edu

Abstract

The paper discusses the problems of cyber-attacks on supply chain management systems in different sectors and industries. It causes high severity and economic losses. Along with various technical terms, the countermeasure technique, both theoretically and in application, are discussed. If developed countermeasures are applied in every sector, it will reduce the cyberattack problem on supply chain management systems. It will create more job opportunities, more secure information, more awareness among people, and more economic generation for any country.

Keywords

Supply Chain Management, Cyberattack, Countermeasures and Economic generation

Introduction

1.1 Supply Chain Management

It is defined as managing everything like the materials, information and services used in the process(es) that are concerned with the supply chain and its associates. Supply chain is a crucial factor in manufacturing of a material.

1.2 Cyberattack

A cyber-attack can be termed a value chain attack in which an infiltration from an outside source tries to access the system and misinterprets the data. It is one of the risks on the supply chain creating a loss of public resources and bringing various levels of structural instability to the organization and the public.

2. Problem/ opportunity explored: Risks in management of supply chain due to cyberattack?

2.1 Research questions/ Objectives

1) How to prevent cyberattacks in supply chain management in different sectors?
2) How to catch up with cyber attackers while managing the supply chain?
3) How to develop a managing technique for self-proofing the supply chain against cyberattacks?

2.2 Methodology

Step 1: This review is done by searching conference papers and journals from Google Scholar and MavScholar, an online search platform by the Minnesota State University, Mankato (MNSU) library. While searching in Google scholar regarding my assigned topic of research, it showed about 22k papers including articles from conference and journals. So, I customized my search years from 2000 to 2022 available on the left side control panel, then it started showing around 17.5k papers. This amount of paper was reduced to 17.2k papers when the search year is from 2010 to 2022. The summary from the papers is in discontinuous form. Information is first taken from the keywords and then sorted as per the relevance of the given topic. Similarly, data from Mavscholar are taken from articles, books, magazines, videos, maps, and newspapers in addition to journals and conference paper.

Step 2: The flowchart for screening of paper for literature review is as shown:

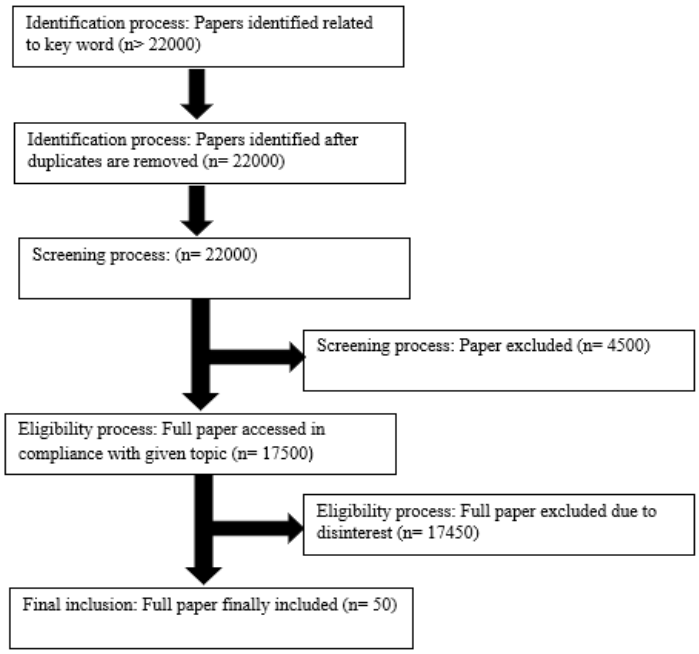

Figure 1. Flowchart for paper screening

3. Literature Review

The main challenges regarding the supply chain lie in the complex processes which need to be correctly understood and manifested to create better awareness of damages to supply chain residents. This is important to properly implement the supply chain network, creating an amplitude of the proper objective of critical mapping areas of the impact of supply chains.

This is vital to create a better modeling network and proper simulation to understand and bring better reflection to help channel the impacts. This is vital in creating better internet infrastructure networks to make this scenario. The criticality again lies in cyber security that needs to be adapted towards managing the risk and creating a proper channel that will be backed by disruptions and creating networks which means channeling and bringing forth the correct amplitude of vulnerabilities that need to be directed. Cyber-attacks are an essential way to understand the conduct of businesses that will improvise in creating a better network and henceforth create better intelligence that will bring a system of business implications (Moghadasi, 2022). This vital point is essential to mitigate the risk and help in crisis readiness in quantifying the cyber risk exposure.

The various threat scenarios need to be channelized, which should motivate the ethical implications of strategies that will help create better rules on cyber risk exposure. The understanding again lies in the factors, desired outcomes, vulnerable groups, and susceptible factors of attacks. We are managing the supply chain risk, which is essential to create a network of security and better business continuity that will improve communication and reduce the crisis. Thus, creating a proper infrastructure will help in computer security and make the benchmark that will improve and better understand cyber-attacks. The different forms of cyber-attacks create this institutional change in getting the right objective that will help ensure other deliverables that need to be implied to create a better network of risk mitigation. This can be done by creating a crisis management plan and proper techniques system to help reduce the risk (Warren, 2000). This is important to create a strong defense channel that will help create a system to strengthen cyber security and create a scenario that will improvise the attacks at various levels. The supply chain services must understand the regulations to create a network that will improvise and bring forth sensitive information to be categorized.

This is vital for proper entities that need to be fixed towards creating a better benchmark of system integrity and distribution of appropriate channels of a management process. The understanding again lies in creating a proper audit and system purpose that will help control a good network for business and help towards cyber threats and growing implications of a process deployment. This is vital for creating an internet layer to help sustain information and generate transparency between entities to address cyber security breaches.

The threat of supply chain cyber-attacks has been growing prominently for a couple of years. Treacherous cyber-attacks have compromised different IT services from Russia to the US in various agencies, creating privacy issues for thousands of customers. Understanding other cyber-attacks like ransomware, which affected thousands of service losses, is essential. The different forms of these attacks happen, one where the criticality of creating a better understanding of the cyber-attacks needs to be understood. This is vital for creating a proper account of supply chain management which would bring the correct users of an electronic system (Lee 2021).

The widespread use of computer systems makes the system dependent and creates a network that will delay the risk of fraudulent activities. Proper customer service management and security alignment must create a better network and reduce physical damage. This is important to develop software dependency and appropriate security alignment methods. This is important to channel the better way of creating a network to help bring better information transition. Several types of attacks, like denial-of-service attacks, create the framework where system processing needs to be aligned—developing a better resolution of the system and processes essential to create a network of customer validation.

This will reduce the use of proper supply chain management in creating better customer collaboration. The steps to minimize computer security risk are essential to channel the better way to adapt towards the different securitization standards. This is important to bring forth better research and improve the technical aspect of the system. This can improve supply chain management and adapt to creating information. This information categorization is essential to help forth different risks of security and improvement and bring the channel that will help in adaptive thought of information categorization. This is vital for making sure of a better adaptation and creating a thought process that will help channel the way of information determinations.

Good services and creating functionality are essential to help bring forth better security standards that will adapt towards the organization process of computer validation. The battle point again lies in making the proper achievement of a system that will help categorize a better network and approach toward comprehensive levels of supply change. The supply chain elements should understand the various way to be capable and bring forth proper digitization of industry 4.0 standards (Marciano 2022).

Industry 4.0 standards create the supply chain organization to improvise and distribute their products. It also adds apps to words indicating the Internet of things, cloud analytics, and creating a framework of operation that will diversify towards creating proper enterprise solutions. This is one way of improving cyber security networks and creating a thought process towards better efficiency and responsiveness. This brings forth an appropriate method of creating data collectability and predictive maintenance to help in the adoption of a better SIM security risk. This adoption is essential to create a better channel of information categorization and to bring forth the better ability of logistics services that need to be adapted. Proper demand management is necessary to develop a better method of security channeling and bring along an understanding that will help in the cognitive bias of flex management. The plan should ensure better operation and implementation that will categorize different ways to reduce cyber-attack vulnerability and create a better direction to help grow the organizational process. This development is essential to help understand the components of cyber securitization. This scenario is vital to help in a better way to create a network of better initiatives and distribution that can be adapted towards making sure of future subsequent management (Tsiamas, 2021). This way of creating a network of helping to better system processes and hardware supply chain and equip them with the proper adoption of network communication to bring forth a better allocation of security systems. This process and alignment will create a better benchmark that will provide appropriate initiative and fulfill the idea of better performance (Tomas Plėta 2020).

Cyber spying and malware are a constant threat to companies using digital technology to increase productivity. Organization management software like Enterprise Resources Planning (ERP) helps a lot in scheduling tasks and enhancing service. Still, on the other side, it provides means for security lapses due to customization options despite strong security plans by the companies, cybercrime attacks like denial of service, web hacking and defacement,

malware, spam, and phishing through these lapses. On a similar line, cybercrimes can happen in supply chain management systems, so an Information Systems (IS) security framework is needed to prevent such attacks. To do this, qualitative data are collected through an online survey from the administrators and stakeholders of supply chain management using the IS framework. The survey found out are as follows: 1) Problem in control of rules, responsibilities, and policy; 2) Implementation of IS framework at various levels of decision-making in the organization. Awa ring of the employee also is vital for the success of the framework. All factors related to IS framework success are interrelated and depend on decision-making practices. Through these efforts, people at the organization will be fully conscious of not sharing passwords, disclosing critical information, and other such acts, hence ensuring safety. Technical countermeasure such as access control, intrusion detection, and managerial awareness helps supply chain management row positively (Mark Wolden 2015).

An information system is used by Maritime port infrastructure for collaborating with other ships during the ship journey or when the ship is near the port. This also generates signals for securing the infrastructure system through graph analysis and risk assessment. It also tells us about the loopholes in the system where cyber-attack can happen. The current attack graph generation method is incapable of dynamic supply chain management as they do not consider entry and target points, propagation length, and the location and capability of the attack. So, a discovery method is implemented which uses constraint and depth-first search with real data for effective protection. The future scope of this work can be used for 1) mitigating cyber-attack by giving strategic defense options and 2) predicting future attacks from previous attack data and its trends (Nikolaos Polatidis 2018)(Nikolaos Polatidis 2018). Cyber attackers nowadays regularly affect any big multinational company's supply chain through its delicate links.

Due to the complex network and for marketing purposes, supply chain information is shared in the open platform, which makes it vulnerable to attack, causing economic loss and brand failure. So, a resilience system against cyber-attack needs to be developed. Various existing systems in the dimension of cyber risks and their resilience system is searched, which will be helpful in both theory and its application. The article has suggested the following recommendation for creating a cyber resilience supply chain system in addition to empirical identification and quantification, which are as follows: 1) Developing a theory of unfolding cyber risk and its resilience in the supply chain; 2) developing application and technique; 3) generating case studies; 4) different kinds of cyber-attack identification; 5) defining keys ways for cyber-attack management; 6) Searching of cyber risks should be done in the distributed form in place of central form and 7) In necessity, rearrangement of resources and contingency plans should be done (Estay 2015).

Climate change has diverted our attention toward sustainability. As the supply chain is a major part of our life economically, a thought to develop sustainable supply chain management is needed. The goal for sustainability, as defined by the united nation globally, can be used in this direction. As we know, the manufacturing supply chain produces poisonous gases and creates imbalance in the natural system, affecting the surroundings socially and economically. Big Data Analytics (BDA), a part of Information and communication technologies (ICT), can identify unsustainable elements in supply chain management and make necessary corrections. Toulmin's argumentation model is implemented to research concern topics and summarize them. From this study, elements of BDA, such as data processing, analytics, reporting, integration, security, and economics, are known. On a similar line, sustainable supply chain management features were discovered: transparency, sustainability culture, corporate goals, and risk management (Mageto 2021).

The report tracks cyber-crimes on supply chain management in federal banks from when information systems were used for business purposes. The damage gets transferred from the bank to its customers resulting in a loss of profit four times. Mostly it has affected those customers who do not have any alternative bank supplier. The damage can be dealt with through internal liquidity buffers and increased borrowing through bank credit lines. It also leads to the rearrangement of affected suppliers or the finding of alternative suppliers by the customer. The reports also discuss the cyber-attack by Russia on Ukraine at its different infrastructures, which affected Ukraine's economy globally, especially during the Covid epidemic (Matteo Crosignani 2021).

Failure Mode, Effects, and Critically Analysis (FMECA) are used to identify and prioritize Supply Chain Risks to reduce critical losses due to the absence of control of risks. At first, risk assessment is explored, and a detailed list of risk in the automotive industry is organized to determine popular risks; Secondly, standby methods to calculate Risk priority number is suggested inside the framework of FMECA through the collaborative Multi-Criteria Decision Making (MCDM) method. A novel calculation process called Analytic Hierarchical Process was used to get factor

weight, then a fuzzy Decision-Making Trial and Evaluation Laboratory was used to find the dependence factor among risks. While planning disruption for preventing or mitigating main concern is given to - 1) Natural disasters affecting the supply chain, 2) manufacturing resources, human utilization, strategy, and its associate's methods, and 3) unfit transportation (Ilyas Mzougui, 2020). This paper investigates popular cyber threats like inference attacks, password sniffing/cracking software, spoofing attacks, denial of service attacks, and direct attacks to recognize supply chain cyber issues. It is needed to create information security automation and finance on human resources such as standardized screening/ employment processes, continuous education system, efficient reward system, and autonomous communication channels about security issues. Top officials in organizations and government agencies are needed (Pak 2011).

Covid 19 pandemic has given a lot of challenges in the healthcare sector, high-end detection techniques, precise equipment, and safety measures like using masks, sanitizer, hand washing with soaps, and online consultation through telemedicine. Apart from that, most academic institutions and healthcare organizations have become vulnerable to cyber-attacks. The international and national regulatory bodies need to ponder solutions to cybercrimes such as looting confidential data relating to Covid 19 vaccine development, modeling, and experimental therapeutics. To do this, academic institutions and healthcare organizations need to be informed, protected, and prepared to act against cyber-attacks (FHEA 2020).

The safety in the cyber world for the generation of efficient and safe biopharmaceuticals can be done through awareness of different stakeholders like industry, government, and healthcare providers. The drawbacks in current and future biomanufacturing trends need to be focused on as it depends on counter-measuring the intellectual property, cyber-physical systems and government-regulated production environment, and high-end manufacturing models. The following steps are done to achieve the goal: 1) analysis of the flow of information digitally in the biopharmaceutical value chain for manufacturing; 2) focus on cybersecurity risks emerging from continuous and distributed systems of advanced manufacturing models and 3) give solutions to mitigate risks.

It helps to implement advanced defensive principles, frame new development, establish permanent security culture that is adaptive to future challenges and maintain transparency needed for the controllable production of efficient and safe medicine (Donovan Guttieres 2019). Energy companies are the recipients and beginners of innovations and fundraisers in the energy sector. It is also a crucial economizer for any country. It also helps to create value-added services for customers using e-solution to problems. The Internet of things and big data analytics are important aspects in this direction, but it also has brought negative impacts like cyber-attack on the energy supply chain and its management. An agile principle related to energy firms' logistics is developed to countermeasure attacks of cybercrimes. It leads to the following results. First, research helps in developing the trend in management science, and second, recognition of risks related to innovation helps in practical application. A relative comparison needs to draw in between energy firms utilizing framing-dominant business models and weak signal methodology in contrast to traditional business models (Dobrowolski 2021).

Recent development in power electronics technologies has helped to popularize Electric Vehicle. The power electronics hardware used in EV charging and associated infrastructures is vulnerable to attacks related to data integration. Various case studies related to cyber-attack are focused on these forms: 1) interference of the chief charger controller and its data based on FPGA logic; 2) setting up hoax communication between the charging controller and other electronic control units and 3) interference with the function of the battery management system. Quality-wise investigation shows are required security measures are taken during the design of charging architecture, and any electrical hazard or damage to a component's health can be prevented to a high amount during hostile cyberattacks (ASHWIN CHANDWANI 2020).

The Internet of things has led to huge growth in the digitalization of production plants and their supply chain at different manufacturing companies. It has helped in the betterment of assembly data, high yield in operation, efficient transmission, and total manufacturing production. It has also helped in the improvement and high efficiency of storehouse computerization. The efficiency in the logistics of products and their transportation is increased by manipulating the shortest way in the least time used during inventory management. The goal of Industry 4.0 is to decrease the involvement of human workers and to focus on automation systems. Still, Industry 5.0 aims to get high benefits through balanced human-machine interaction. Repeated tasks in the manufacturing industry can be done efficiently and accurately through robots but these robots need human hands to solve problems encountered. Internet of Things (IoT) will also help the industry in the betterment and increasing economy. Consumers will get the advantage

of the technology at reduced prices and continuous supply. Apart from the manufacturing industry, this concept can be implemented in transportation, power, and energy-based industries, including the smart industrial sectors (Zainab Fatima, 2022). Previous analysis has shown that cyber security cannot be fully done by using Firewalls, antivirus software, and other technology for the protection of personal data and computer networks. The awareness about cyber ethics, cyber safety, and cyber security needs to be raised early in the education sector. The features of getting security from cybercrimes are technology, operation and awareness, training, and education (Priti Saxena 2012).

4. Results

The literature reviews the problems of cyber-attacks on supply chain management systems in different sectors and industries. The countermeasure technique, both theoretically and in the application, has developed and needs to be applied in every sector.

5. Discussion

My finding on a cyberattack on supply chain management systems in different industries and relative sectors is that it causes high severity and economic losses. Society needs to be more aware of this topic through online resources, debates, quizzes, and other marketing platforms. The future of counter-measuring the cyber-attack in supply chain management is very advanced as it will create more job opportunities, more secure information, more awareness among people, and more economic generation for any country.

6. Conclusion

This piece focuses on remodeling and resolution making of network for the supply chain after a cyber-attack in which crucial services are lost. The administrator is the chief in charge of taking any resolution for the restoration of the supply network. The modeling is done in two steps: 1) Determining the previous damages by the administrator to get the complete data; 2) Randomly determining programming which involves different recovery cases. Using a literature survey, a real case study is developed. The results of steps 1 and 2 are contrasted, which shows that the deterministic model in an unpredictable case does not generate good solutions; hence a stochastic programming model is suitable in uncertain cases (Emily A Heath 2018).

References

Ashwin Chandwani, . m., *ieee open access*, 1-17, 2020.

Dobrowolski, Z. , . Internet of Things and Other E-Solutions in Supply Chain Management May Generate Threats in the Energy Sector—The Quest for Preventive Measures. *energies*, pp. 1-11, 2021.

Donovan Guttieres, S. S., Cyberbiosecurity in Advanced Manufacturing Models. *frontiers in Bioengineering and Biotechnology*, 1-8, 2019.

Emily A Heath, J. E., Models for restoration decision making for a supply chain network after a cyber attack. *Journal of Defense Modeling and Simulation: Applications Methodology, Technology*, 1-15,2018.

Estay, O. K. (2015, April 16). Supply Chain Cyber-Resilience: Creating an Agenda for Future Research. *Cyber-Resilience in Supply Chains*, pp. 6-12.

FHEA, M. M. (2020). Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. *International Journal For Quality In Health Care*, 1-4.

Ilyas Mzougui, S. C. (2020, june 10). Assessing Supply Chain Risks in the Automotive Industry through a Modified MCDM-Based FMECA. *processes*, p. 22.

Lee, R. D. (2021). New York Department of Financial Services Questions Its Regulated Entities on Responses to and Lessons Learned from the SolarWinds Cyberattack. *Computer and Internet Lawyer*, 16–20.

Mageto, J. (2021). Big Data Analytics in Sustainable Supply Chain Management: A Focus on Manufacturing Supply Chains. *sustainability*, 22.

Marciano, M. B. (2022). *A Geopolitical Lens for Cyber Resilience.* Retrieved from In BCG Insights. Boston Consulting Group Boston, MA.

Mark Wolden, R. V. (2015). The effectiveness of COBIT 5 Information Security Framework for reducing. *IFAC* (p. 7). Montreal: Elsevier.

Matteo Crosignani, M. M., *Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chains.* New York: Federal Reserve Bank of New York Staff Reports, no. 937, 2021.

Moghadasi, N. C., Trust and Security of Electric Vehicle-to-Grid Systems and Hardware Supply Chains. *Reliability Engineering & System Safety*, 108565,2022.

Nikolaos Polatidis, M. P., Cyber-attack path discovery in a dynamic supply chain maritime risk management system. *Computer Standards & Interfaces*, 74-82,2018.

Pak, S.-w. C.-s., An Integrative View on Cyber Threat to Global Supply Chain Management Systems. *Journal of Korea Trade*, 55-87,2011.

Priti Saxena, B. K., A Cyber Era Approach for Building Awareness in Cyber Security for Educational System in India. *International Journal of Information and Education Technology*, 1-5,2012.

Tomas Plėta, M. T. (2020). CYBER-ATTACKS TO CRITICAL ENERGY INFRASTRUCTURE AND MANAGEMENT ISSUES: OVERVIEW OF SELECTED CASES. *Insights into Regional Development*, 1-13.

Tsiamas, K. &., A simulation-based decision support system to improve the resilience of the food supply chain. *International Journal of Computer Integrated Manufacturing*, 34(9), 996–1010,2021.

Warren, M. &. (2000). Cyber attacks against supply chain management systems: a short note. *International Journal of Physical Distribution & Logistics Management*.

Zainab Fatima, M. H., Production Plant andWarehouse Automation with IoT and Industry 5.0. *MDPI applied sciences*, 1-34,2022.

Biographies:

Gaurav Ghosh is pursuing his second Master's in Engineering Management at MNSU, Mankato. Currently, he is also engineering intern at TFT Corp. He has done his first Master's in Power and Energy at Amrita Vishwa Vidyapeetham, Kerala, India with Bachelor's in Electrical and Electronics Engineering. He has experience teaching ng undergraduates as faculty in Government Engineering College, Vaishali, Bihar in India. He has also served as a Service Engineer in a franchise of Siemens Healthcare. He has done workshop and training during his studies at electtrical substations, solar energy extraction and its implementation in the airport and the domestic area along with countermeasure technique for digital radio frequency type devices. His research interests consist of renewable energy, manufacturing techniques and supply chain management, electrical vehicle, solid state fabricated devices, quality assurance and heuristic methods. He has also published an article in the International Journal of Pure and Applied Mathematics on "Design of Zero Net Energy Building".

Pawan Bhandari, PhD is an Assistant Professor of Department of Manufacturing Engineering Technology at Minnesota State University, Mankato, USA. He earned a B.S. and M.S. in Manufacturing Engineering Technology from Minnesota State University, Mankato, USA, and his Ph.D. in Technology Management (Quality Systems) from Indiana State University, USA. He worked as a Senior Health Systems Engineer at Mayo Clinic, Rochester, Minnesota where he ovided end-to-end consulting to internal clients from department toto region to the enterprise level. He was also an instructor in Health Care Systems Engineering, the College of Medicine, Mayo Clinic. Prior to joining Mayo Clinic in 2013, he was a Manufacturing Engineer. He is also a member of the American Society for Quality (ASQ) and the Association of Technology, Managementand Applied Engineering (ATMAE). He is also an ASQ Certified Six Sigma Black Belt and ASQ Certified Quality Improvement Associate. His research interests are quality and process improvement, technology management, quality systems, performance improvement in healthcare, and business analytics which includes but is not limited to machine learning, Artificial Intelligence, and data science.