IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, September 2025
Impact Factor: 7.67

Study on Supply Chain Cybersecurity: Risks, Challenges

Dr. J. Joselin[1], Aiswarya S Varier[2], Manoj T[3]
Assistant Professor[1]
BCA Student[2,3]
Sri Krishna Arts and Science College, Coimbatore
joselinj@skasc.ac.in, aiswaryasvarier23bca005@skasc.ac.in, manojt23bca030@skasc.ac.in

Abstract: *As the world grows more interconnected, firms increasingly rely on broad supply chains to conduct business. However, monitoring the supply chain and the risks connected with it is a process that is time-consuming and expensive for many organizations. In many instances, businesses that do not appropriately manage the risks associated with their supply chain are more likely to become victims of a cyberattack, which has the potential to cause significant disruptions in their operations. In this article, we will take a more in-depth look at supply chain risk management, the dangers that are most commonly associated with it, as well as the five actions that your company can take toward worry-free supply chain risk management.*

Keywords: *Supply chain, Cyber Security, Risk Management*

I. INTRODUCTION

The term "Supply Chain" represents the interfusion of physical and technological systems among networks. With this interfusion, there is increased production, organization, and profitability. The main features of a supply chain are independent activities that are independent of location, deep integration, a variety of automated services, and the capability to react to customers' needs and requirements in a contextual fashion. The term "intelligent supply chain systems" was coined in association with the emergence of Industry systems, mainly to indicate the fourth industrial revolution and the integration of intelligent systems into supply chain processes. These systems provide support to both the industry and military sectors by facilitating production and manufacturing processes. They place particular emphasis on the exchange of models and information within worldwide networks, while also ensuring their secure management. Supply chains play a very important role in businesses by enabling the accomplishment of core procedures and logistical requirements. In the context of military operations, supply chains have a function that goes beyond mere profit-oriented goals. Rather, they have the potential to deliver major results that are vital to the success of missions and the survival of human life. Modern society has created a fundamental dependency on computer networks enabled by industrial systems, which are vital for different digital activities in everyday life. This dependence, therefore, subjects society to potential cyber weaknesses, especially when such systems are breached by sophisticated cyber or physical hacking techniques. The area of research aimed at the improvement and prevention of cyber-attacks is an area of international interest. The capabilities of both nation states and non-nation states are continuously developing and advancing. At the same time, supply chains are facing an increasing trend towards increased efficiency, interconnectedness, and digitalization. The correlation between supply chains that are facilitated by digital technology and the escalating militarization of the cyber domain is a research area of considerable importance. The growing reliance on computing and communications infrastructures is causing significant transformations in the functioning and integration of supply chain processes. The potential ramifications of exploiting a weakness inside a military supply chain extend beyond economic implications, posing a significant risk to human life. With the wide-ranging purchase of defense products The global offensive surface for malicious players has increased, resulting in the potential for magnifying the negative effects resulting from a cyber-attack on supply chain systems. The basic principles of the global supply chain

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 1, September 2025 Impact Factor: 7.67

increasingly depend upon the use of the internet and network connectivity. The existence of this interdependence has consequential implications for the security and effectiveness of these systems. The global supply chains are being re-emphasized in their importance and their vulnerability as a potential target is being implicated because of numerous factors like changes in the operational environment, technological advancements, and alterations in the maintenance of systems and platforms. Supply chain risk is a term used to describe the sudden probability that affects the macro- or micro-level dimensions of supply chain processes, leading to repercussions for various elements of supply chain operations, such as Information Technology (IT) and Operational Technology (OT). Risk management is an important process that entails the forecast and evaluation of cyber threats so as to determine and mitigate possible risk incidents, thus lowering their impact. This strategy would be of great use in explaining the cyber threats that supply chains face. The categorization of supply chain risks includes two methodological approaches, i.e., interruption and operation.

The disruption risk is caused by natural disasters, like earthquake or flooding, and prevention of this type of risk is not an easy task. Operational risk covers different factors, such as cyber-attacks, which relate to inefficient conduct of supply and demand operations during the process of production or distribution of finished goods. The supply chain operations standardization and the mitigation of mission successes can be eased through the development of mission assurance, agile life-cycle engineering, and risk management procedures. Furthermore, it effectively facilitates the implementation of emerging technologies such as blockchain, the Internet of Things (IoT), applications of Artificial Intelligence (AI), and Cyber-Physical Systems (CPS). These technologies make it possible to provide automated and secure services to organizations, thus improving the productivity and flexibility of supply chain activities. The possible influence of mission assurance models on the response strategies of militaries and defense organizations towards Advanced Persistent Threats (APT) could be considerable. The application of multiple concepts, such as crown jewel analysis, business continuity methodology, ontological-based semantic models, service orchestration systems, and the improvement of redundant and degenerate systems or processes, can help facilitate the achievement of improved mission assurance in organizational environments. The effect of the technical environment upon military operations and the likely implications of innovation in this area can heavily affect the effectiveness and efficiency of military supply chain activities. As a result, defense companies are confronting an increasing imperative to have the ability to assess the possible impacts of upcoming technologies on their supply chains, allowing them to successfully include or mitigate any connected risks.

WHAT IS SUPPLY CHAIN RISK MANAGEMENT?

Supply chains are used to denote the complex system linking a corporation with its suppliers, on which the company relies for the production and distribution of its products or services. Management of a supply chain involves the supervision of the flow of goods, including the different steps involved in transforming the raw materials used by an organization into the end products or services produced by such company. Supply chain management involves the planning and effective execution of numerous activities connected with the acquisition, procurement, and transformation of raw materials, as well as the effective management of logistical operations. One of the main reasons why companies adopt a global supply chain management strategy is to increase their competitive advantage. The existence of supply chains can create many benefits; nevertheless, it must be noted that they can also increase an organization's risk exposure in relation to quality, safety, business continuity, reputation, and cybersecurity. Since the outbreak of the COVID-19 pandemic, the media spotlight has increasingly been on supply chains, as the effects of supply chain disruptions have touched regular customers everywhere. The pandemic has brought to light the inherent vulnerability of traditional supply systems to these kinds of disturbances. All organizations are vulnerable to both internal and external threats that occur as a consequence of disruptions to their supply chains. The process of managing the likely risks related to such disruptions is widely known as supply chain risk management (SCRM). Supply chain risk management include the systematic identification, evaluation, prioritization, and mitigation of potential threats to the supply chain and the associated risks they provide. Third-party risk management (TPRM) constitutes a crucial element within the realm of supply chain risk management. Firms of all industries typically have dealings with outside entities within their supply

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 1, September 2025 Impact Factor: 7.67

chain, including suppliers, vendors, contractors, or service providers. The intrinsic natures of these economic links of necessity expose these firms to substantial risks. As per empirical data, the average number of third-party suppliers with whom companies share their information stands at around 730. Among the companies that share their data with third parties, a significant 53 percent have experienced at least one data breach attributed to a third party. These breaches have resulted in an average financial burden of almost $7.5 million. In addition to instances of data breaches, external risks within supply chains encompass various factors, such as the impact of unpredictable or misunderstood customer demand, disruptions in the movement of products including raw materials, components, and finished goods, as well as the occurrence of natural disasters like earthquakes, hurricanes, and tornadoes, among others. In addition, internal supply chain risks encompass various factors such as disruptions in internal operations, alterations in key management, personnel, and business processes, non-adherence to environmental regulations or labor laws, inadequate cybersecurity policies and controls to safeguard against cyberattacks and data breaches, and other related concerns. Irrespective of approach, the inclusion of a firm within the supply chain, particularly through the practice of outsourcing to third parties, inherently poses risks to the company. The supply chain exposes firms to a range of potential disruptions, such as legal, compliance, financial, strategic, and reputational risks, which may not be faced in other settings. One of the most important risks that the supply chain poses to companies is the cyber threat, which involves the likelihood of a cybersecurity incident causing an interruption in data and business operations. In light of the increasing reliance on third-party entities by organizations and the concurrent rise in cybersecurity incidents, it is imperative for organizations to develop and execute a comprehensive supply chain risk management strategy. This approach is vital in protecting the company, its customers, and any other business relationships against potentially disastrous cybersecurity threats inherent in the supply chain.

WHAT ARE THE TYPES OF CYBER RISKS IN SUPPLY CHAIN MANAGEMENT

As previously said, cyber risk is a growing concern that supply chains provide to enterprises. Unfortunately, most companies working within the supply chain are likely to face disruptions in terms of data, financial, or operational issues at some point. The effects of these disturbances on your company will depend upon the success of your supply chain risk management plan. The growing digitization of the business ecosystem requires the use of numerous digital technologies like the Internet of Things (IoT) and Industrial Internet of Things (IIoT) to improve supply chain operations in businesses. But, the arrival of these new technologies also makes companies susceptible to new cybersecurity threats, such as but not limited to malware, ransomware, phishing, and hacking. Data breaches, cybersecurity attacks, and malware and ransomware attacks are common threats that companies face in their supply chains in modern times. Then, a deeper analysis will be made of each of these cyber threats, explaining the possible harmful effect they can have on your business.

Data Breaches

Data breaches are an important and serious cybersecurity threat faced by modern businesses.The likelihood of an upsurge in both the quantity and intensity of these security breaches is great in the near future. When an organization experiences a data leak or data breach, it usually causes enormous economic losses and reputational damage, in addition to possible regulatory and legal consequences. The average cost of a data breach in the year 2021 was a significant amount of $4.2 million. Even with the appropriate regulatory and compliance frameworks in place, organizations are often experiencing considerable delays in uncovering data breaches after they have taken place. Studies indicate that the average time taken to identify a data breach is about 197 days. Furthermore, the above number also goes up when companies experience a data breach because of a supply chain security risk. In a joint study by IBM and the Ponemon Institute, it was found that a corporation takes an average of 280 days to detect a third-party data breach. The possible manifestations of this phenomenon include intellectual property as well as personally identifiable information (PII). Some common data breaches by third-party vendors are illegal access via company email addresses, email provider hacking, lack of encryption, unsecured websites and misstored login details. In some cases, it is even possible for third parties to knowingly reveal confidential customer data to outside

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 1, September 2025 Impact Factor: 7.67

parties, exposing your organization to possible supply chain attacks that are coordinated by cybercriminals, hacktivists, and even hostile nation-states.

Cybersecurity Incidents

The scope of this category is intentional, as it covers a set of new technologies that put enterprises at risk of increased vulnerability to attacks in their supply chains, in ways previously unknown. In the modern era, the use of web-enabled devices creates possible threats in the supply chain.The Internet of Things (IoT) typically include consumer-oriented devices, such personal fitness trackers and smart thermostats. As of 2021, the global count of active IoT devices exceeded 10 billion. The term "IIoT" primarily pertains to the utilization of equipment for powering organizations on a significantly greater scale. The reason for the Industrial Internet of Things (IIoT) is to make industrial processes better by connecting different devices that are networked and can communicate via the Internet. These range from sensors and scales to engines and elevators. These technologies facilitate the enhancement of organizational efficiencies, encompassing reduced time to market, improved asset monitoring across the supply chain, cost reductions, and the establishment of safer workplaces, among other benefits. Additionally,these technologies create a number of cybersecurity weaknesses for the organizations that use them. Cyber criminals are conscious of the less-than-optimal security condition in the IoT and IIoT areas, making them more vulnerable to cyberattacks. Based on statistical data on IoT-based attacks in 2019, it was observed that the average duration between the activation of an IoT device and the occurrence of an attack was approximately five minutes. In the context of Industrial Internet of Things (IIoT) devices utilized in industrial systems, the ramifications of a cybersecurity breach can have far-reaching and severe implications. These include but are not limited to the following: disruption of production processes,financial repercussions, unauthorized access and theft of sensitive data, substantial harm to equipment, acts of industrial espionage, and potential physical injury to individuals.

Malware and Ransomware Attacks

The prevalence of malware and ransomware attacks is regrettably increasing. The primary objective of these attacks is to illicitly acquire information, manipulate internal data, or obliterate confidential information. Malware is a type of intrusive software with the ability to infiltrate computer systems in order to destroy or damage them, or to steal data from them.The prevalent forms of malware attacks encompass viruses, worms, Trojans, and ransomware. The SolarWinds malware attack of 2020 stands out as a highly notable incident within the realm of previous malware assaults. In the first stages of the year, the systems of SolarWinds, a corporation headquartered in Texas, were compromised by cybercriminals who inserted malevolent code into the organization's software system known as Orion. This particular program was extensively employed by approximately 33,000 clients for the purpose of overseeing their information technology assets. In March 2020, SolarWinds sent software updates to its customers via the Orion platform, unwittingly carrying the malicious code that had been planted by the attackers. Later, the virus created a hidden backdoor within the information and communication technology infrastructure of SolarWinds' customers, thus facilitating the cybercriminals to use more malware with the aim of underground surveillance on those organizations and companies. Ransomware is a common type of malicious software attack. This specific form of malicious software uses encryption methods to lock the files of its victims, thereby allowing the attacker to extract money in exchange for a decryption key. In most cases, the monetary transaction with a decryption key for recovery of data is made using cryptocurrencies like bitcoin, with the aim of hiding the identity of the criminals. The year 2021 witnessed a ransomware attack targeting Colonial Pipeline, resulting in the temporary cessation of the company's activities for a number of days. Consequently, this incident precipitated a scarcity of gasoline throughout the southern region of the United States. The hackers first gained unauthorized access to Colonial's computer networks by using a virtual private network (VPN) account, which was meant for remote employee access to the network. But the virtual private network (VPN) did not use multi-factor authentication as a prerequisite for entry. As a result, the attackers were capable of entering Colonial's network by using a compromised username and password. It is highly

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 1, September 2025 Impact Factor: 7.67

probable that this login information was obtained through a data breach that revealed an employee's credentials. Finally, Colonial paid the cyberattackers a total of $4.4 million as a form of quid pro quo for having provided a decryption key to enable the recovery of their stolen data. However, because of the slow response of the decryption key, the company was forced to rely on its in-house backup processes in an effort to restore the delivery of services. Later on, Colonial Pipeline was able to resume its operations; however, it suffered severe negative impacts on its operations, ranging from several financial and reputational implications.

ANALYSIS ON FIELD OF STUDYCOVERED IN WOS AND SCOPUS DATABASE

In the analysis of the whole final selected articles after screening, the researchers found areas of studies pertaining to cyber security within the context of supply chain management. When most companies and businesses think about security, they often think about securing their digital networks, software, and assets from cyber attacks and data breaches. But, for the supply chains of whether traditional manufacturers or service providers, or data supply chains trusted by most large companies, they are also vulnerable to security risks. This is seen in many big data breaches through third parties. In practice, every company or business has a place in the supply chain, where the supply chain continues to grow on the flow of information such as the flow of goods and services. Thus, it is not surprising that supply chain security is an extremely complex and constantly changing function. Then, this indicates that business leaders are more alert as the threats to information throughout the supply chain become more evident.

Network Security

According to Gaigole and Kalyankar, network security is a critical component for computer users as well as business organizations. In addition, safety is the foremost issue with the extensive use of the internet. There is no denying the fact that the internet itself can bring about certain security threats. This is made clear when the intellectual property can be easily accessed via the internet, and numerous types of attacks can be sent over the network. There are variations in network security management for every kind of scenario, and it is required because the expanded daily usage of the internet involves home or office usage, where it needs underlying protection. But big companies need high maintenance, capable software, and advanced hardware to avoid hackers and scammers. On the contrary, Gaigole and Kalyankaremphasized that network security must be a concern to the whole network, for it to remain awake and secure. Network security does not only focus on computer security at each end of the communication network, but it should also be monitored when sending data, as communication channels should not be vulnerable. This is due to the fact that it will threaten more. The hackers can be planning to break into communication lines, acquire, and manipulate data, and spread false information in the network.

Web Application Security

Jain and Parashu described that there is a need to protect any software that is used by the user. Any of these programs could have holes or weaknesses where an attacker can inject user requests. Apart from this, application security encompasses software, hardware, and procedural means to secure applications and prevent external threats. In addition to other things, elements of application security also comprise measures taken during the development life cycle to secure applications from potential risks through vulnerabilities. It encompasses the design, development, utilization, upgrading, or servicing of applications. In addition, the security regulations included in security forms and procedures in the correct use of applications can reduce the chances of manipulation of applications to pilfer data, hacking words to open up access, and taking control of the data held. Pandey and Singh [2020] categorize cyber security threats into three types: cyber security, supply risk, operational risk and demand risk. Cyber physical system has driven global innovation into the SC professionals' day-to-day operations. Web applications are a critical class of service provider and communication medium for users. Vulnerability on the internet can produce detrimental effects and influence all sensitive data. In addition, the principal cause of this is that developers have limited programming skills and lack awareness of the importance of cyber security.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, September 2025
Impact Factor: 7.67

Information Security

Information security is defined as a collection of methods for controlling the tools, rules, and processes that are used in identifying, avoiding, and recording. Besides, it is also used to counteract threats towards digital and non-digital information. The reason for establishing an information security programme is to safeguard the integrity, availability, and confidentiality of a company's information and data and its information technology system. Among others, it is also to make sure that sensitive data are released only to the authorities, prevent manipulating garbage data, and ascertain whether the right authorities can view the data when necessary. The establishment of information security programs seeks to safeguard the integrity, availability, and confidentiality of business data systems and information technology.

II. CONCLUSION

In an era of rising global interconnectedness, companies are increasingly dependent on expansive supply chains to facilitate their operations. However, the monitoring process of the supply chain and its related risks is an arduous and expensive task for a number of companies. In numerous cases, enterprises that fail to effectively mitigate the risks connected with their supply chain are at a higher probability of falling prey to a cyberattack, hence leading to substantial interruptions in their operational activities. This article aims to provide a comprehensive analysis of supply chain risk management, focusing on the typically associated hazards and proposing five recommended measures that organizations can undertake to address these concerns. The concept of supply chain risk management, which involves the identification, assessment, and mitigation of potential risks within a supply chain, has gained significant attention in recent years. Organizations are increasingly recognizing the importance of effectively managing risks that may disrupt the flow of goods. The future course of Social Customer Relationship Management (SCRM) will be marked by an increased focus on managing third-party risk, wider adoption of Artificial Intelligence (AI) and Machine Learning (ML), greater use of blockchain technology, increased regulatory scrutiny, and the introduction of new technologies and solutions. Organizations that demonstrate proactive measures in adjusting to these developments will be more effectively positioned to mitigate the risks associated with their supply chain and uphold the comprehensive security of their operations. In summary, firms who use these methods are more likely to enhance their business growth and maintain a competitive advantage over their rivals.

REFERENCES

[1]. https://www.researchgate.net/publication/374661353_Supply_Chain_Cybersecurity_Risks_Challenges_and_Strategies_for_a_Globalized_World
[2]. https://www.researchgate.net/publication/350496787_Cyber_security_in_supply_chain_management_A_systematic_review
[3]. https://fepbl.com/index.php/ijmer/article/view/1241
[4]. https://www.sciencedirect.com/science/article/pii/S1366554520308590