International Journal of Computer Trends and Technology
ISSN: 2231–2803 / https://doi.org/10.14445/22312803/IJCTT-V73I6P105

Volume 73 Issue 6, 34-41, June 2025

Original Article

Understanding Cybersecurity Risks in Supply Chain Management

Rajender Pell Reddy

Cybersecurity Advisor, Richmond, VA, USA.

Corresponding Author : rpellreddy@gmail.com

Received: 26 April 2025 Revised: 30 May 2025 Accepted: 14 June 2025 Published: 28 June 2025

Abstract *- This document globalization has put SCM at high cybersecurity risk, undermining information operations and security. The present paper explores various facets of cybersecurity risks associated with SCM, such as the issues related to the supplier's network, lack of strong encryption policies, and the surge of hi-tech cyber threats. We review academic literature, present methodologies of risk identification risk management measures and focus on examples of SC attacks that demonstrate supply chain risk impacts in actual scenarios. A suggested causal analysis plan covers cybersecurity threats and utilizes the application of technological tools like the blockchain, machine learning, and zero-trust architecture. Last of all, we touch on the need to promote the culture of cybersecurity for all actors involved.*

Keywords *- Supply Chain Management, Cybersecurity, Blockchain, Zero-Trust, Cyber Threats.*

1. Introduction

1.1. Importance of Supply Chain Management

Supply Chain Management (SCM) is an essential business function that deals with the administration of the efficient flow of products, services, information and capital through many intermediaries within a supply chain. Suppliers' sources include the procurement of raw materials, production process, inventory control, final product distribution to customers, and delivery. [1-4] Supply chain management is one of the key components of any organization because it determines how efficiently products and services get to the end-users. Below are six key subheadings that elaborate on the importance of SCM:

1.1.1 Cost Efficiency and Optimization:

Another focal area regarding the strategies of SCM is to minimize operational expenses. Therefore, optimal procurement, production and distribution operations can help businesses minimize waste and costs while improving operations and production. Most notably, supply chain management helps organizations take advantage of buying, appropriation, inventory holding, and transportation costs since it provides economies of scale.

If, for instance, firms adopt low-cost strategies, including time stocks, they will be in a proper position to meet their customer's demands without having to stock unnecessary items that will cost them much money and take up much of their space a factor that is likely to boost its profitability as well as sale prices.

Fig. 1 Importance of supply chain management

1.1.2. Customer Satisfaction and Service Delivery

Customer satisfaction is a key factor in today's highly competitive market, and SCM is important to fulfilling customer expectations. Effective supply chain management aims to deliver products and services in the shortest time possible, which means that lead times are cut and the availability of goods is increased. Holding efficient stock records, proper routing strategies, and real-time tracking through information technology helps to improve the service delivery that was manifested by delivering the order to the customers at the right time. Another advantage of SCM is that it allows firms to respond effectively to customer needs by quickly changing their strategies, resulting in improved demand and preference.

1.1.3. Risk Mitigation and Resilience

Many risks can affect the supply chains, such as natural disasters, political instabilities, economic fluctuations and cyber risks. Thus, when picking up the opportunities and threats of a specific SCM approach, possible risks, corresponding contingency plans, and ideas for flexible strategies must be identified. A flexible supply chain may run uninterrupted and relatively efficient even in the face of external disturbances, meaning it will deliver its products in the shortest time possible. It shows that handling suppliers, developing safety stock, and implementing disaster recovery plans help reduce disruption risks affecting supply and supporting organizational sustainability.

1.1.4. Global Reach and Competitive Advantage

Today, SCM is necessary for companies that seek to function internationally, as globalization has broadened supply chains. A fully incorporated supply chain allows organizations to acquire global resources from leading suppliers, take advantage of cheap production costs, and reach a wider market. This approach lets companies achieve higher competitiveness through lower costs of goods, access to locally unavailable materials, or increased differentiation of their products. SCM also assists companies in managing regulatory difficulties regarding international standards, customs, and import/export laws.

1.1.5. Innovation and Product Development

This paper elucidates that effective SCM ensures the provision of real-time information between various production stages so businesses can embrace the development of new products. Closely linking with suppliers and manufacturers, the company gets access to current materials, technologies, and production methods that result in the development of new products. Further still, SCM enables the organization to respond to the dynamic market and customer needs and demands by adapting the production plans or plans for goods to reflect new changes. The supply chain innovation strategy can provide a company with excellent market coverage and make its products stand out among similar products of other players in the field.

1.1.6. Sustainability and Environmental Impact

Therefore, with increasing concerns over environmental factors and changing customer preferences, SCM is critically responsible for enhancing environmentally sustainable systems. ZF explicitly uses the term triple bottom line and aims to minimize companies' carbon footprint through efficient transport routing, reduced packaging, and sustainable purchasing. Besides compliance with rules and regulations, green supply chain practices like energy-efficient manufacturing, recycling, and waste minimization contribute to the company's CSR goals. This paper establishes that sustainable sourcing enhances organizational image and consumer appeal and reduces long-term business social costs on the environment.

1.2. Cybersecurity Challenges in SCM

Cybersecurity threats affecting SCM have evolved and escalated to high levels, posing immense dangers to organizations' operations. Due to the increased globalization of operations, supply chains have become long and vulnerable, third parties are involved in crucial operations, and all these factors create many opportunities for attackers. A tough question is the issue of piracy, where hackers may break into an organization's system to steal a valuable product design, research, a unique process or a trade secret, thus creating an unfavorable position for the organization. Piracy of materials can significantly harm a business, both in contemporary competitive share and in further potential for expansion. Another of the most significant cybersecurity threats is operational disruption due to multiple cyberattacks like ransomware. In ransomware attacks, threat actors lock an organization's important data to ensure they make a payment for the decrypting key. These attacks can stop business processes, slow down the shipment of products, and paralyse customer support services. Ransomware attacks threaten to cost the victim an upfront amount of lost productivity, and the demanded ransom engenders long-term image and credibility damage. [5,6] Cybersecurity risks include another form of attack known as phishing attacks in SCM. In phishing, hackers lure employees or supply chain partners into releasing confidential information, including usernames, passwords, or monetary information. In other cases, the attacker disguises or mimics legal entities or people to achieve the goal, obtain access to internal systems, or control the transactions' flow for illicit ends.

One of the significant issues with phishing in supply chains is that it often operates on the employees of the companies involved, contractors, or suppliers rather than the technology and addresses social engineering factors. Moreover, Advanced Persistent Threats (APTs) are one of the more silent and prolonged cyber security threats. APTs are long-duration and complex attack techniques in which the attackers compromise a supply chain network space and remain undetected. These attacks are mostly for espionage, stealing sensitive information, and disrupting other data and

computer processes for wrong intents. APTs can be challenging to detect because they operate stealthily and are selective; it is even worse for big organizations with their supply chains spread cross-nationally. These cybersecurity challenges in SCM are worsened by the growing dependencies of organizations with their suppliers, whereby one challenge in the entire network leads to a chain reaction effect on other comparable companies in the supply chain. Therefore, organizations must invest in strong cybersecurity defences to ensure they do not fall victim to these threats, strengthen monitoring, threat intel sharing, and employee and partner cybersecurity education.

2. Literature Survey

2.1. Overview of Cybersecurity in SCM

Supply chain security has gained importance in Supply Chain Management (SCM) due to a rapid increase in companies adopting supply chain networks. The World Economic Forum's report of 202 was insightful, with a projection that forty-five percent of cyberattacks focused on supply chains due to their strategic nature as links in the global economy. [7-10] Supply chain cyber risks threaten business operations, erode credibility and are costly. These positions require extensive and flexible cybersecurity measures to protect against attacks effectively. Increasing integration of supply chain members and the centrality of digital technologies enhance the call for efficient and effective risk management strategies of these key supply chain systems.

2.2. Cyber Threats in Supply Chains

The cyber threats range in a way that targets the supply chains, given that their structures are complex and are mostly veiled. Ransomware continues to be particularly disruptive, as cybercriminals lock up core processes and operational data and demand payment to unlock it and resume operations. Phishing attacks are another common type; an attacker may send an email or a message that mimics a legitimate supply chain partner and request login details, authentication credentials or any other sensitive details; in the process, the whole network may be infiltrated and attacked. Moreover, IT-near insiders, including motivated employees, corporate spies, or personnel targeted through 'social engineering,' are dangerous due to access granted to the core organizational assets. These threats underscore that risks in SCM are diverse and dynamic in terms of cybersecurity.

2.3. Existing Mitigation Strategies

Different approaches have been implemented to mitigate the supply chain's cybersecurity risks. Blockchain technology has proved to be very effective in making supply chain transactions transparent, and this has made the record generated here completely tamper-proof; hence, a lot of trust developed among different stakeholders of an organization. Multi-factor authentication, MFA as commonly referred to, provides an important layer of security since multiple factors must be used before entry into the system is allowed, thereby restricting the chances of the system being compromised. Furthermore, it contributes to an organization's capability of successfully preventing and managing an incident by implementing incident response plans. While these plans describe detailed action procedures that enable organizations to minimize harm, recover operations, and conduct post-incident investigations, they also minimize downtime and possible losses. In aggregate, these approaches define a platform for protecting supply chains from threats in the cyber domain.

2.4. Research Gaps

However, as the findings reveal, a vast research area still exists despite the developments in cyber risk management; more crucially, systematic and highly flexible ISRM concepts are absent for SCM. Recent research mostly examines single technical interventions without exploring the integration of these tools in various supply chain environments. Besides, the measure of human risk and the extent to which people are vulnerable in supply chain cyber security are not well understood. Such oversights stem from careless mistakes, ignorance and lack of proper training among supply chain members, but very scant literature exists on how to manage these problems. Closing these gaps requires a more complex strategy that involves the application of both technologies and human solutions to make supply chains sustainable and protectable.

3. Methodology

3.1. Research Design

Therefore, this study follows a mixed-method approach that enables the researcher to understand cybersecurity risks in SCM. This paper uses quantitative and qualitative research approaches to understand the research topic comprehensively. This type of research comprises the gathering and evaluating numerate information strictly associated with cyber-attacks, weaknesses, and protection measures amidst supply chain networks. [11-16] This makes it easy to develop trend, pattern and correlation analyses that offer a big picture of the cybersecurity threats.

Quantitative and qualitative data is collected with the help of supply chain managers, cybersecurity professionals, and policymakers through interviews and focused discussions. These viewpoints of experts bring practical insights into real-life issues, cognitive approaches to problem-solving and real-life application of security solutions. The integration of these methods guarantees a comprehensive and diverse analysis of the cybersecurity threats, which are still lacking in SCM's theoretical references and everyday uses.

3.2. Data Collection

3.2.1. Primary Data

The main data source for this research was interviews conducted on potential primary supply chain and cybersecurity informants. Participants comprised those who

control the supply chain, cybersecurity specialists, and technology suppliers, each with a different point of view on what problems and solutions concern cybersecurity threats. The interview questions were mainly formulated to provide specific questions mixed with overarching ones. They allowed for the consideration of concrete experiences, approaches, and attitudes, which yielded some useful first-hand information about the practicalities of cybersecurity management in SCM.

3.2.2. Secondary Data

This secondary research data was obtained from reliable manufacturers' case studies, industry journals and publications, and academic articles. Best practices showed explicit descriptions of examples based on experience with the consequences of cyber-attacks and the success rate of the implemented safeguards.

Industry reports also provided information on new trends, threats, and measures to protect the supply chain. They presented theoretical concept articles and data-driven articles that provided knowledge to undergird the research. These secondary data sources were useful and supported the primary data to provide a rich, consistent analysis throughout the research.

3.3. Proposed Framework

3.3.1. Threat Identification

The framework consists of three layers appropriately used to determine cybersecurity vulnerabilities in SCM.

Network Analysis

Instead, the network analysis concentrates on recognizing the weak links in the supply chain's information technology structure. This is the process of identity divulging operation that aims at performing thorough searches in a network to determine the potential points of failure in the network, exposed devices, outdated equipment, or insecure transmission paths. Regarding this, network analysis can draw a network topology scheme and expose the lines of possible threats, which creates the basis for protecting critical resources and adopting proper measures.

Behavioural Analysis

Behavioural analysis identifies activities deviating from normal behaviour, indicating an invasion is underway. This layer of analysis detects deviations from normal operations by always checking the patterns of users and systems, such as the time of login by unauthorized users, baptism of new personnel or any other strange activity that may be captured in the test. Sophisticated tools building upon machine learning take this process further because they can pick up on almost undetectable anomalies and link them to specific dangers, creating a risk prevention system of early warning signs.

Threat Intelligence

Threat intelligence combines cyber threats and feeds sharing platforms to address continuing risk factors. This tier uses data from threat databases, sector-focused bulletins, collaborations and research for new threats and weaknesses. Incorporating this intelligence in the supply chain's cybersecurity plan helps the organisation remain vigilant and appropriately change its protection mechanisms and responses to further threats.

3.3.2. Risk Assessment Model

The risk assessment model employed in this study is derived from a risk formula that considers two factors: the probability of an incident occurring in the supply chain and the compelling force of the event if it were to occur. The likelihood factor is obtained from past events, such as previous cyber-attacks, threats particular to the industry type and the general trends in cybersecurity infringements. This analysis also helps to calculate the likelihood of different types of attacks like ransomware, phishing or insider threats so that an organization can prioritize potential risks. The effect is calculated based on probable losses in terms of finance and functionality in case the network is compromised. This comprises the cost of the ransom demand, fines, cost of business disruption, reputational costs, and others. The overall formula with these two variables yields a straightforward risk measure that enables a supply chain manager to determine the most urgent cybersecurity risks to confront.

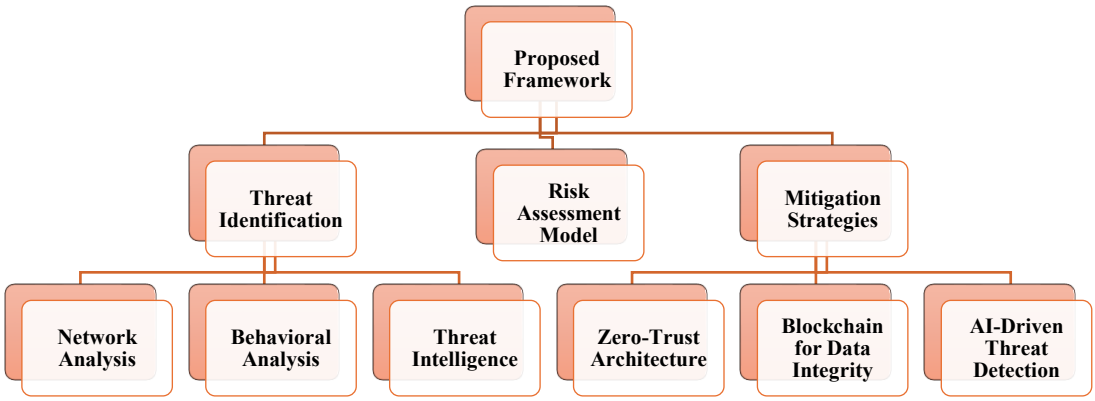

Fig. 2 Proposed framework

3.3.3. Mitigation Strategies

Zero-Trust Architecture

Zero-trust architecture is a security structure that implements various mechanisms based on the expected security principle of never trusting and always verifying. Here, the opening of the resources within the supply chain network and their availability to the users and devices is selective. This strategy presupposes that internal and external networks are equally fragile, so users must constantly present their credentials before being allowed to access any system or information. This way, zero-trust reduces the likelihood of unlawful access or internal threats, making it a strong part of the supply chain cybersecurity model.

Blockchain for Data Integrity

Blockchain technology brings significant benefits in increasing the quality of data within the supply chain. Blockchain maintains an Institutionalizing tamper-proof transaction record, the chain of source records that documents every activity, every exchange or change of something, or every transaction in the supply chain environment. This decentralized system helps keep track records intact and sealed so that once information is entered, it cannot be faked or erased without detection. Hence, it affords protection against cybercrimes such as faking records or fraud. It also leads to increased transparency to enable the accrual of data that, when shared with the other stakeholders, the latter can independently verify the transaction, which creates trust in the chain.

AI-Driven Threat Detection

AI-based threat analysis mechanisms are the strategies that reverse engineer and plan cyber intrusions before they take place. Such systems always scan the traffic patterns, the usage of the network by users and the systemic performance for anomalous behaviours. In real-time data handling, AI can discover patterns and deviations from one's normal operations that can signify a cyberattack, like unauthorized attempts to gain access or abnormally large volumes of data transfers out of place. The AI models learn about new and developing threats and improve themselves in identifying new complex attacks. This preventable measure helps organizations act quickly and solve emerging problems, thus limiting the effects of possible breaches on a supply chain.

3.4. Validation Techniques

Reliable and effective validation technology paved the way for validating the proposed framework. This framework, which used simulation models to analyze cybersecurity scenarios in real supply chain networks, was further verified. These models normally represent how supply chain networks may behave and may contain a mix of characteristics such as stakeholders, functions and tools that may be incorporated. [17,18] Using multiple simulations and threat scenarios such as ransomware attacks, phishing attempts, and internal threats, it was possible to reevaluate the framework's chance of detecting, measuring, and resisting such threats. Besides the simulations, the framework was validated in various supply chain contexts to evaluate the flexibility and effectiveness of the framework in various operational environments. Such scenarios considered supply chain scale and challenges requiring the framework's implementation, extending it across manufacturing logistics, retail, and others.

The approach of using several scenarios proved valuable in establishing the general feasibility of the framework to function in any given supply chain setting. In these validation techniques, the framework was validated to confirm the discernment of risks, measurement of the impact and the capability to implement the right safeguards in different operational contexts. Information from the simulations and scenarios helped improve the framework, and the results were quite valuable.

4. Results and Discussion

4.1. Case Study Analysis

4.1.1. Target Data Breach (2013)

The specification of ways cybersecurity risks in supply chains can escalate can be illustrated with the Target data breach. One of Target's third-party suppliers received an email intended to deceive them, which gave the attackers access to Target's payment system. This breach affected the personal data of more than 40 million customers, resulting in a loss of reputation and enormous financial losses.

The primary lesson that can be learned is the need to perform periodic assessments of external partners' security measures. Supply chains are systems that depend largely on third parties or other organizations, and hence, any weaknesses inherent in the partners' systems will ripple through the organization's systems. Therefore, suppliers must continue exhibiting an acceptable level of cybersecurity to the organization.

4.1.2. Maersk Ransomware Attack (2017):

In 2017, Maersk, one of the world's biggest logistics firms, fell to rampant ransomware attacks that closed down its operations on several continents. It is estimated that the attack cost the firm $300 million because it affected its functioning and disrupted the supply chain. The effect was worst felt because the attack targeted the company's core operational systems, disrupting ports and logistics functions. Two significant things that organizations, especially technical organizations, must learn from this incident include incident response plans and data backup. However, its recovery was not easy for one simple reason: Maersk lacked backup solutions and was initially unprepared for a cyberattack. The following measures to minimise the impact of this type of malware and reduce its downtime should be taken: clear and rehearsed response procedures to this particular threat, and should make sure that their data is regularly backed up.

4.2. Simulation Results

4.2.1. Simulation Scenario 1

Implementation of Zero-Trust Architecture

The simulated supply chain network noted a 60% improvement in the cases of unauthorized access due to the integration of zero-trust architecture. Here, only authorized users and devices gained access to the sensitive systems and data secure from external and internal threats. The simulation showed that by making cumbersome and consistent security measures, it is possible to minimize the risks of leakage of information and threats to employees.

4.2.2. Simulation Scenario 2

Blockchain Adoption for Data Integrity

Other simulations for protecting transactional information, such as the application of blockchain technology, enhanced the tracking of supply chain exercises. This led to a 45 percent reduction in fraud activities as the blocks self-check, and it is almost impossible for attackers to manipulate the previous records. When the simulation was complete, it brought to light how the blockchain attributes of openness and its protected nature could boost the reliability and veracity of all data to every stakeholder in the supply chain.

Table 1. Simulation results

Simulation Results	Percentage
Implementation of Zero-Trust Architecture	60%
Blockchain Adoption for Data Integrity	45%

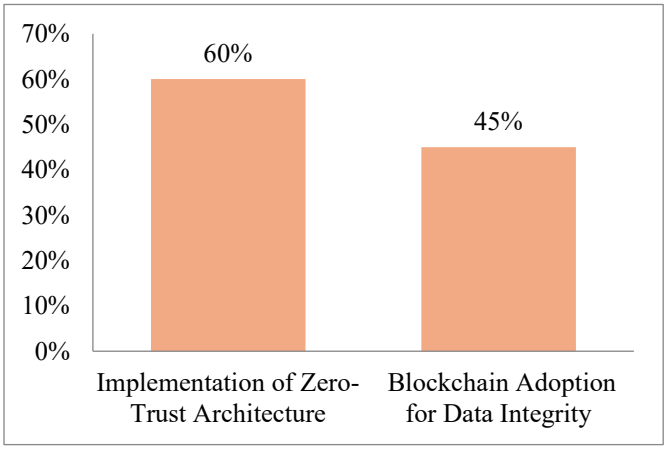

Fig. 3 Graph representing Simulation Results

4.3. Discussion

The case study analysis and the simulations showcase that the human factor is crucial in supply chain cybersecurity. L4, utilising state-of-the-art approaches such as zero-trust architecture and blockchain, considerably lowered primary threats, namely, illegitimate entry and scams. However, the results also reveal the need for good governance, which features frequent auditing, well-formulated incident response protocols, and multi-sectarian cooperation. Although incorporating these technologies is mandatory, it has high initial costs for infrastructure and training, particularly for relatively small organizations within the supply chain zone. However, using such systems may not be easily integrated since the partners may be unable to invest in such solutions. Hence, there is a need for cross-industry work where large firms can help smaller supply partners implement better practices and technologies. With an active environment established through supply chain cooperation, the risk from growing and evolving cyber threats can be mitigated.

5. Conclusion

Cybersecurity has emerged as one of the core competencies of sustainable SCM, where safeguarding information, assets, and business processes from current and future cyber risks is not an option. Based on this research, the following are ten indications pointing to adopting cybersecurity in SCM. First, threat identification has the critical function of addressing threats that can arise concerning cyber risks. One can prevent and deal with emerging threats using network analysis, behaviour analysis, and intelligent threat analysis. Secondly, building up a more effective risk assessment model assists organizations in assessing the risks imposed by cyber threats and their probability degree and possible damages, which can allocate resources and countermeasures in a timely manner. The simulations performed in this paper's research demonstrated that contemporary technologies, including zero-trust architecture and blockchain, can boost the cybersecurity readiness of supply chains. In contrast, the zero-trust model decreased the risk of unauthorized access by 60%; blockchain shrank fraud instances by 45%. Such observations highlight the possibility of implementing the layered approach: using technological solutions and recognizable risk management tools to guarantee the reliable protection of supply chain networks against cyber threats.

5.1. Recommendations

The following recommendations could be made from the study to improve cybersecurity in the supply chain. First, organizations must provide their employees with training to raise awareness. It is interesting to note that human factors are still a major contributor to the cybersecurity problems of executives and organizations, as well as phishing attacks and internal threats. In this, employee training and creating awareness of the most probable threats are must-take steps toward minimizing the risks. Moreover, organizations should consider adopting a zero-trust model first and then using blockchain technology. The zero-trust principle means every request that comes in has to be validated, thus significantly reducing the possibility of someone coming in with the wrong intention; on the other hand, blockchain puts much emphasis on data integrity by coming up with records of the transaction, which are transparent and are in most cases cannot be altered. All of these technologies can effectively help build the

security of the supply chain. Last but not least, it is crucial that businesses carry out periodic checks on the supplier's level of cybersecurity. An example studied by Target showed that weaknesses in third parties can significantly impact the supply chain's strength.

Benchmarking suppliers against a set of cybersecurity metrics ensures that partners stay secure and minimize the risk of disruption.

5.2. Future Research

Future studies should identify new risks and countermeasures for applying supply chain cybersecurity. One is the explication of the threats of quantum computing on supply chain security. This technology can disrupt areas like encryption, and knowing how quantum can change current systems is important for predicting new threats to cryptographic systems. However, there is a lack of literature on generating comprehensive cybersecurity essentials that SMEs can adopt on a large scale. Larger organizations, on the other hand, could easily integrate and implement such technologies into the organization because of their resources; SMEs may experience some difficulties in the same. Flexible and relatively inexpensive architectures that can be designed for the end customer, concerning the specifics of SMEs, will be the foundation for a successful supply of cybersecurity for the entire supply chain. The recent developments in these areas will offer insights into how the security of future supply chains can be enhanced.

References

[1] Sara Saberi et al., "Blockchain Technology and Its Relationships to Sustainable Supply Chain Management," *International Journal of Production Research*, vol. 57, no. 7, pp. 2117-2135, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[2] Shipra Pandey et al., "Cyber Security Risks in Globalized Supply Chains: Conceptual Framework," *Journal of Global Operations and Strategic Sourcing*, vol. 13, no. 1, pp. 103-128, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[3] Claudia Colicchia, Alessandro Creazza, and David A. Menachof, "Managing Cyber and Information Risks in Supply Chains: Insights from an Exploratory Analysis," *Supply Chain Management: An International Journal*, vol. 24, no. 2, pp. 215-240, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[4] Mari Aarland, "Cybersecurity in Digital Supply Chains in the Procurement Process: Introducing the Digital Supply Chain Management Framework," *Information & Computer Security*, vol. 33, no. 1, pp. 5-24, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[5] Jason Deane, Wade Baker, and Loren Rees, "Cybersecurity in Supply Chains: Quantifying Risk," *Journal of Computer Information Systems*, vol. 63, no. 3, pp. 507-521, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[6] Federico Del Giorgio Solfa, "Impacts of Cyber Security and Supply Chain Risk on Digital Operations: Evidence from the Pharmaceutical Industry," *International Journal of Technology, Innovation and Management*, vol. 2, no. 2, pp. 18-32, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] Zhang Wei, and Wu Xiang, "The Importance of Supply Chain Management," *International Journal of Business and Social Science*, vol. 4, no. 16, pp. 279-282, 2013. [Google Scholar] [Publisher Link]

[8] Steven A. Melnyk et al., "New Challenges in Supply Chain Management: Cybersecurity across the Supply Chain," *International Journal of Production Research*, vol. 60, no. 1, pp. 162-183, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] Theresa Sobb, Benjamin Turnbull, and Nour Moustafa, "Supply Chain 4.0: A Survey of Cyber Security Challenges, Solutions and Future Directions," *Electronics*, vol. 9, no. 11, pp. 1-31, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[10] Oluwabunmi Layode et al., "Addressing Cybersecurity Challenges in Sustainable Supply Chain Management: A Review of Current Practices and Future Directions," *International Journal of Management & Entrepreneurship Research*, vol. 6, no. 6, pp. 1954-1981, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] Om Pal, and Vandana Srivastava, and Bashir Alam, "Cyber Security Risks and Challenges in Supply Chain," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, pp. 662-666, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[12] Naeem Firdous Syed et al., "Traceability in Supply Chains: A Cyber Security Analysis," *Computers & Security*, vol. 112, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] Luca Urciuoli et al., "Supply Chain Cyber Security–Potential Threats," *Information & Security: An International Journal*, vol. 29, no. 1, pp. 51-68, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[14] Isaac Daniel Sánchez-García, Jezreel Mejía, and Tomás San Feliu Gilabert, "Cybersecurity Risk Assessment: A Systematic Mapping Review, Proposal, and Validation," *Applied Sciences*, vol. 13, no. 1, pp. 1-29, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[15] Andrew Fielder et al., "Risk Assessment Uncertainties in Cybersecurity Investments," *Games*, vol. 9, no. 2, pp. 1-14, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[16] Valentina Petrova, "A Cybersecurity Risk Assessment," *International Scientific Journal "Industry 4.0"*, vol. 6, no. 1, pp. 37-40, 2021. [Google Scholar] [Publisher Link]

[17] Yuanhang He et al., "A Survey on Zero Trust Architecture: Challenges and Future Trends," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, pp. 1-13, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[18] Nishant Kumar et al., "Blockchain Adoption for Data Integrity in Higher Education E-Learning," *International Conference on Data Analytics for Business and Industry*, Sakheer, Bahrain, pp. 1-6, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[19] Avijit Roy, Anik Dhar, and Sejuti Sarker Tinny, "Strengthening IoT Cybersecurity with Zero Trust Architecture: A Comprehensive Review," *Journal of Computer Science and Information Technology*, vol. 1, no. 1, pp. 25-50, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[20] Vinden Wylde et al., "Cybersecurity, Data Privacy and Blockchain: A Review," *SN Computer Science*, vol. 3, no. 2, pp. 1-12, 2022. [CrossRef] [Google Scholar] [Publisher Link]