Implementation of Cybersecurity in Protecting for Cyberattacks

Alessandra Valentina1, Kenny Budiarso Lawson2, Sabrina Nurul Azmi2

1,2,3 Faculty of Engineering and Informatics, Multimedia Nusantara University, Tangerang, Indonesia

Accepted on mmmmm dd, yyyy

Approved on mmmmm dd, yyyy

*Abstract*—The use of supply chains has been applied to almost all industries such as information technology, pharmaceutical industry, energy, manufacturing, military, logistics, retail, government, and even finance. The security aspect is one of the important things in implementing the supply chain so that there are no cyber attacks on data. However, attacks often occur that damage the supply chain network. Attacks from the supply chain also vary, such as viruses, phishing, and self-interested insider attacks. These attacks have a domino effect on a very complex and integrated supply chain. Therefore, this research will examine more deeply the cybersecurity approaches applied in protecting the supply chain from cyber attacks, what are the critical factors in maintaining its security, as well as identify challenges and solutions in implementing cybersecurity. The method used is Systematic Literature Review which reviews 294 literatures related to the implementation of supply chain protection from cyber attacks. As a result of the review, there were 30 articles related to the topic. This research contributes to providing insights related to implementing cybersecurity in protecting the supply chain from cyber attacks so that companies are more aware of cyber attacks that have a detrimental impact.

Index Terms—cyberattacks; cybersecurity; supply chain; systematic literature review

# Introduction

In the era of many technologies, the use of supply chains has been applied to almost all industries such as the Information Technology Industry, pharmaceutical and health industries, energy, manufacturing, military, logistics, retail, government, and even finance. Each sector has different business processes depending on the type of service. The implementation of the supply chain must be based on strong security, especially from cyber attacks. However, cyber attacks often occur in this sector, especially those related to data such as data theft to data sabotage [1], [2]. Furthermore, the company still relies on technology or networks of suppliers, distributors, and other third parties, especially those with high vulnerability, so that a cyber attack can successfully penetrate the security, causing significant damage that threatens the company's business ecosystem and economy as a whole [3], [4], [5], [6].

Cyber attacks on the supply chain cause operational disruptions that affect the company's finances and reputation in the eyes of other business partners. If it lasts for a long time, it will affect consumer and market loyalty, and damage data that hampers innovation, especially in emerging industries such as the pharmaceutical and healthcare industries for the development of better patient and drug services [7]. This must be supported by the coordination of various parties, sophisticated cybersecurity technology, and good security management from the company. This aims to increase company security and minimize potential losses.

Cybersecurity is designed to protect systems, networks, and digital data from unauthorized access, theft, and damage and includes techniques, processes, and practices to safeguard sensitive information and prevent cyberattacks [8], [9]. Cybersecurity covers various aspects such as data protection, management of access rights, detection and action against cyber attacks, and planning to respond to cyber-attacks. In the supply chain, cybersecurity is one of the crucial concerns, especially in an integrated digital system [10]. Cyberattacks can cause losses, especially to data, finances, and company operations. To reduce these risks, organizations must implement a good security framework and management through a collaboration of various parties such as vendors, and operators for communication for transparency so that no miscommunication causes conflict in the operational process.

Cyber attacks in the supply chain through various means such as through viruses including ransomware, and phishing, as well as insider attacks by exploiting the company's dependence on complex supply chains [2]. Because the supply chain system is integrated, these attacks have a domino effect on the network as a whole. As in the case of SolarWinds in 2020, there were security vulnerabilities in the supply chain with 15-97% of the source code coming from third parties, indicating that cyberattacks had infiltrated the process in the form of viruses that spread rapidly through infected networks [11]. This undermined public confidence in Orion, the developer of SolarWinds.

With good cybersecurity technology and management, cyberattacks can be prevented so that the company's reputation does not falter in the eyes of other business partners and can serve consumers quickly and in real time. Various literature studies have been conducted by collecting articles from multiple sources to explore approaches taken to protect the supply chain from cyber attacks. However, the solutions implemented also bring multiple challenges such as security risks that continue to grow as technology advances, complexity in the implementation of the supply chain, and other challenges that have an impact on company operations, especially in supply chain management. The purpose of this study is to examine more deeply through a Systematic Literature Review (SLR) related to cybersecurity approaches applied in protecting the supply chain from cyber attacks, as well as identifying challenges and solutions that arise in implementing cybersecurity.

# Method

## Search Process

## 

This research uses the PRISMA method by collecting previous articles as a literature study to support the implementation of this SLR. The initial stage began with determining keywords, namely cybersecurity, cyberattack, and Supply Chain Management. Through these keywords, 294 articles were obtained from the Scopus database using the Publish or Perish tool. Furthermore, the articles were filtered based on title and abstract, resulting in 68 relevant articles. Of these, only 30 articles were available in open access, which were then used as the final reference for this SLR.

## Inclusion and Exclusion

This research applies inclusion and exclusion criteria as a systematic step to screen the literature studies used. By applying these two criteria, the resulting literature studies are expected to be highly relevant, reliable, and optimally support the main objectives of the research. Table 1 is an example of the Inclusion and Exclusion criteria applied in this research.

1. Inclusion and Exclusion Criteria

|  |  |
| --- | --- |
| Inclusion Criteria | 1. Only written in English. 2. Publication range 2020 – 2024. 3. Related to topic. |
| Exclusion Criteria | 1. Publication not open access. 2. Publication out of range. |

## Research Question

Based on the problems related to the supply chain, research questions were formulated to answer these problems:

1. How can multi-actor collaboration in the supply chain effectively enhance cybersecurity?
2. What is the impact of technology usage on transparency and data security in supply chain management?
3. How can the integration of AI and IoT optimize real-time response to cybersecurity threats?
4. What are the key factors influencing the effectiveness of risk mitigation strategies in the context of cybersecurity within the supply chain?

## Tools

This research utilized three main tools to support the process of preparing the Systematic Literature Review (SLR):

1. Publish or Perish: Used to collect literature studies based on selected databases, such as Scopus, making it easier to find relevant articles.
2. Microsoft Excel: Used for various activities such as checking for duplication of articles, sorting journals based on certain criteria, and organizing data systematically.
3. Mendeley: Served as a reference management tool that facilitated the citation process and bibliography management in this study.

The use of these three tools helped ensure that the SLR process was structured, efficient, and well-documented.

# Result and Discussions

The results of the review have been carried out on 294 articles, 30 articles are relevant and open access. Based on these 30 articles, there are main factors why supply chain management can be implemented, namely as follows:

1. The use of Quantum Computing which offers a significant increase in data processing speed is critical in addressing increasingly complex cyber threats. Coupled with incident response time optimization, companies can respond to threats faster, minimize potential losses, and increase system resilience.
2. Strong collaboration between various stakeholders, including operators and suppliers, is key to the success of secure SCM. By standardizing security processes and transparent communication, this collaboration enables better risk management. In addition, the integration of data security using technologies such as blockchain and strong encryption increases trust between parties involved in the supply chain.
3. Strong Data Security with Encryption and Cybersecurity Management. Strong data security is the foundation of secure SCM, especially with the implementation of hybrid encryption and cryptography technologies. This protects sensitive data from hacking and unauthorized access. Coupled with effective cybersecurity management, companies can implement a comprehensive solution to mitigate threats across the supply chain.
4. Implementation of Blockchain and Digital Twin Technologies to Increase Visibility. Blockchain not only offers transparency and traceability but also enables data decentralization, which increases system reliability and reduces the risk of fraud. The integration of Digital Twin technology helps in real-time simulation and modeling of the supply chain, enabling companies to identify potential issues faster and make better decisions to improve visibility across the supply chain.
5. Integrated Risk Management and Cybersecurity with Customized Architecture. Using an integrated cybersecurity architecture, including an automated risk management solution, SCM can be designed to proactively detect, respond to, and prevent cyberattacks. The use of a comprehensive security framework and the implementation of international standards ensure higher system resilience to cyberattacks.

With these factors, supply chain management cyber attacks can be prevented so that the company's ecosystem is protected both from data and information to delivery and relationships with suppliers. This will affect sustainable reputation and customer trust. Because, without strong security, it is very vulnerable to attack by irresponsible parties the continuity of company operations is disrupted. However, some challenges must be faced in implementing the supply chain, especially in supply chain data security, which are as follows:

1. Security incident complexity and supply chain vulnerabilities. Fragmented supply chains increase the risk of vulnerabilities, making security incidents complex and difficult to handle, as an attack at one point can affect the system.
2. Difficulty managing real-time data and addressing cyber threats. Real-time data management and rapid response to cyber threats is a challenge, because the volume of data is very large, especially since the pattern of cyber attacks can change to become more sophisticated in the ever-evolving digital era. This is homework that companies must face in anticipating these attacks.
3. Cryptographic vulnerability management and security compliance. Complex encryption processes and cryptographic key management can slow down supply chain management transactions. Ensuring compliance with security standards across multiple jurisdictions also adds to the challenge.
4. Technology implementation and cyber integration. Implementation of new technologies such as blockchain often faces resistance, as well as technical challenges in integrating legacy systems with modern cyberinfrastructure.
5. Resource and infrastructure limitations. Many organizations face resource and infrastructure limitations to address dynamic cyber threats, leading to a lack of visibility and adequate oversight.

These challenges must be overcome if they cannot be overcome, then the security of the supply chain network that has been built is vulnerable to various cyber attacks, especially complex and integrated supply chain systems. If one part is attacked, it will affect other parts and can even spread quickly. Therefore, support from various parties is needed in facing the challenges that exist. In addition, the findings of the literature study will be presented in the form of the following table.

1. Study result

| No. Ref | Author | Paper Title | Year |
| --- | --- | --- | --- |
| 1 | *Manuel A.* [12] | Minimizing incident response time in real-world scenarios using quantum computing | 2024 |
| 2 | Tania Wallis [13] | Implementing Partnerships in Energy Supply Chain Cybersecurity Resilience | 2023 |
| 3 | Krishnamoorthy N[14] | Implementation of Cloud Computing Data Security Based on Hybrid Elliptical Curve Cryptography | 2023 |
| 4 | Vasiliu-Feltes I [7] | Impact of Blockchain-Digital Twin Technology on Precision Health, Pharmaceutical Industry, and Life Sciences | 2023 |
| 5 | Masip-Bruin X [15] | Cybersecurity in ICT Supply Chains: Key Challenges and a Relevant Architecture | 2021 |
| 6 | Altaleb H [16] | 5G Evolution and Supply Chain Security in MENA Region: Challenges and Opportunities | 2024 |
| 7 | Segal G [17] | A Blockchain base computerized network infrastructure | 2023 |
| 8 | Gupta N [18] | Additive Manufacturing Cyber-Physical System: Supply Chain and Risks | 2020 |
| 9 | Ibiyemi & Olutimehin [10] | Cybersecurity in supply chains: Addressing emerging threats with strategic measures | 2024 |
| 10 | Farah, B [19] | A survey on blockchain technology in the maritime industry: Challenges and future perspectives | 2024 |
| 11 | Olubunmi [1] | Strategies for Protecting IT Supply Chain Against Cybersecurity Threats | 2024 |
| 12 | Mohd Nasrulddin Abd Latif [3] | Cyber Security in Supply Chain Management: A Systematic Review | 2021 |
| 13 | Joash Mageto [20] | Big Data Analytics in Sustainable Supply Chain Management: A Focus on Manufacturing Supply Chains​ | 2021 |
| 14 | Tadeusz Sawik [21] | Balancing Cybersecurity in a Supply Chain Under Direct and Indirect Cyber Risks | 2021 |
| 15 | Abel Yeboah-Ofori [22] | Mitigating Cyber Supply Chain Risks in Cyber-Physical Systems Organizational Landscape | 2019 |
| 16 | Badis Hammi [23] | Security Threats, Countermeasures, and Challenges of Digital Supply Chains | 2023 |
| 17 | Michael Herburger [24] | Building Supply Chain Resilience to Cyber Risks: A Dynamic Capabilities Perspective | 2024 |
| 18 | Sara Abbaspour Asadollah [25] | Enhancing Cybersecurity Through Comprehensive Investigation of Data Flow-Based Attack Scenarios | 2024 |
| 19 | Sana Al-Farsi [26] | Security of Blockchain-Based Supply Chain Management Systems: Challenges and Opportunities | 2021 |
| 20 | Xinyuan Wang [4] | On the Feasibility of Detecting Software Supply Chain Attacks | 2021 |
| 21 | Tadeusz Sawik [27] | A Linear Model for Optimal Cybersecurity Investment in Industry 4.0 Supply Chains | 2020 |
| 22 | Sana Al-Farsi [28] | Securing Blockchain-Based Supply Chain Workflow Against Internal and External Attacks | 2022 |
| 23 | Zachary A. Collier [29] | The Zero Trust Supply Chain: Managing Supply Chain Risk in the Absence of Trust | 2021 |
| 24 | Niloofar Etemadi [5] | Supply Chain Disruption Risk Management with Blockchain: A Dynamic Literature Review | 2022 |
| 25 | James Pérez-Morón [30] | Eleven Years of Cyberattacks on Chinese Supply Chains in an Era of Cyber Warfare, a Review and Future Research Agenda | 2021 |
| 26 | Darrell Norman Burrell [31] | Supply Chain and Logistics Management and an Open Door Policy Concerning Cyber Securit | 2020 |
| 27 | Chinenye Okafor [32] | SoK: Analysis of Software Supply Chain Security by Establishing Secure Design Properties | 2021 |
| 28 | Motunrayo Oluremi Ibiyemi [10] | Safeguarding Supply Chains from Cyber-Physical System Attacks: Frameworks and Strategies | 2024 |
| 29 | Timothy Kieras [6] | I-SCRAM: A Framework for IoT Supply Chain Risk Analysis and Mitigation Decisions | 2021 |
| 30 | Theresa Sobb [33] | Supply Chain 4.0: A Survey of Cyber Security Challenges, Solutions, and Future Directions | 2020 |

**RQ 1: How can multi-actor collaboration in the supply chain effectively enhance cybersecurity?**

Multi-actor collaboration in the supply chain is very important in security, especially in supply chain networks that are accessed by various parties. This requires trust and transparency in communication so that no miscommunication can have an impact on the supply chain, especially in terms of security, be it with suppliers, distributors, vendors, regular audits, and related stakeholders who play an important role in supply chain security [13], [15], [18], [20], [22], [25], [26]. Several collaboration strategies can be implemented to effectively improve cybersecurity, including increasing transparency and collaboration between stakeholders securing the software supply chain, providing training on the importance of cybersecurity awareness, implementing blockchain technology for transparency and security, and improving data integrity [2], [4], [19], [27], [28], [29]. In addition, it requires collaboration with customers and partners to entrust their loyalty to the company [6], [33]. Collaboration both in terms of supply chain security and supply chain technology, it helps in mitigating cyber-attacks that continue to grow and vary so action is needed in dealing with these attacks.

**RQ 2: What is the impact of technology usage on transparency and data security in supply chain management?**

The use of technology in data transparency in supply chain management has various significant impacts, some of which are even able to identify suspicious activities, which is one of the important steps in its implementation so that it can be used as a reference in planning for handling cyber attacks. The following are some of the technology applications used in supply chain data transparency.

1. Quantum Computing is used to optimize incident response time as well as risk management automation due to its ability to handle several incidents quickly [12].
2. Cybersecurity Partnership and Assurance Model, a cybersecurity framework with a focus on cooperation between parties in the supply chain to strengthen cybersecurity throughout the network [13].
3. Blockchain and Digital Twin. This model combines blockchain technology for transparency and security, and Digital Twin for simulation and optimization of supply chain processes [7].
4. SCOR (Supply Chain Operations Reference) Model. SCOR is used to evaluate and improve supply chain performance, including processes, metrics, and management practices, as well as software mapping to improve operational efficiency. Through such planning, it can improve operational efficiency that help in saving costs through automation and optimization of processes [5], [6], [26], [30], [33].
5. Big Data Analytics (BDA) and Cyber-Physical Systems (CPS). Integrating BDA for real-time data analysis and CPS for production and logistics optimization, providing end-to-end visibility in the supply chain [20].
6. Zero Trust Supply Chain Model. Assuming that no actor or data flow can be trusted by default, this model relies on strict authentication and real-time monitoring for every supply chain process [29]. This helps in mitigating cybersecurity risks across the supply chain due to the occasional flow of data from actors that are not fully trustworthy.
7. Blockchain-Based SCM Model. This model focuses on using blockchain to secure and improve supply chain transparency, supporting automation with smart contracts. From studies that have been conducted, this model can improve the reliability of data such as medical data, optimize control over access and sensitive data to minimize the risk of fraud, and create better transparency in the supply chain [1], [17], [26].
8. Cyber Supply Chain Risk Management (C-SCRM). This model focuses on mitigating cyber risks in the supply chain, with a focus on collaboration between partners, transparency, and managing risks from third parties. This model provides various benefits such as increased security and stability of the supply chain, efficiency through the use of technology in risk mitigation, and preventing of exploitation and attacks from outside parties that can cause supply chain failures [10], [22], [31].

**RQ 3: How can the integration of AI and IoT optimize real-time response to cybersecurity threats?**

The use of AI (Artificial Intelligence) and IoT (Internet of Things) is certainly a big step, especially in an era that is constantly evolving and starting to automate. The integration of IoT and AI supports real-time response to improve efficiency and visibility in the supply chain [6], [33]. The implementation of both provides various benefits to the supply chain system, including increased efficiency and operational cost savings due to IoT technology that can collect real-time data, increased data security throughout the supply chain, reduced risk of data theft, and better visibility and tracking of products and information [2], [3]. In addition, the use of AI can speed up the detection and response to security incidents so that cyberattacks can be dealt with once detected [2].

**RQ 4: What are the key factors influencing the effectiveness of risk mitigation strategies in the context of cybersecurity within the supply chain?**

1. Leadership and Management Commitment: Support from the organization's leadership ensures adequate resource allocation for cybersecurity [15], [16], [23], [24], [32].
2. Comprehensive Risk Evaluation: Identifying and prioritizing risks within the entire supply chain [13], [23], [24], [25], [26], [32].
3. Reliable Security Technology: Implementation of tools such as firewalls, intrusion detection, and data encryption [1], [3], [12], [16], [17], [19], [20], [21], [22], [32].
4. Collaboration with External Parties: Involving third parties in threat management, such as cybersecurity providers [1], [3], [7], [13], [15], [16], [17], [18], [19], [20], [21], [22], [32].
5. HR Capacity Bulting: Regular training for employees in identifying and handling threats [3], [10], [19], [30].
6. Regulatory Compliance: Ensuring the strategy complies with security standards and applicable laws [7], [14], [16], [19].

CONCLUSION

Strong collaboration between actors in the supply chain, such as suppliers, distributors, and customers, has proven effective in improving cybersecurity. This is achieved through real-time exchange of threat information, implementation of common security standards, and strengthening training and awareness of potential attacks. Technologies such as blockchain strengthen this collaboration by creating transparency and accountability in transactions. The use of modern technologies such as blockchain, big data analytics, and AI has a significant impact on data transparency and security. On the one hand, these technologies improve the reliability of data recording and threat detection capabilities. However, on the other hand, the implementation of technology also presents new challenges, such as the need to protect IoT devices that are prone to attack. The combination of AI and IoT provides an effective solution for dealing with cyber threats in real time. Continuous monitoring by IoT and AI-based predictive analytics enable early detection and automated response to threats. This speed and accuracy reduce the negative impact of attacks on supply chain operations.

REFERENCES

[1] Olubunmi Adeolu Adenekan, Chinedu Ezeigweneme, and Excel Great Chukwurah, “Strategies for protecting IT supply chains against cybersecurity threats,” *Int. J. Manag. Entrep. Res.*, vol. 6, no. 5, pp. 1598–1606, 2024, doi: 10.51594/ijmer.v6i5.1125.

[2] M. O. Ibiyemi and D. O. Olutimehin, “Cybersecurity in supply chains: Addressing emerging threats with strategic measures,” *Int. J. Manag. Entrep. Res.*, vol. 6, no. 6, 2024.

[3] M. N. A. Latif, N. A. A. Aziz, N. S. N. Hussin, and Z. A. Aziz, “Cyber security in supply chain management: A systematic review,” *Logforum*, vol. 17, no. 1, pp. 49–57, 2021, doi: 10.17270/J.LOG.2021555.

[4] X. Wang, “On the Feasibility of Detecting Software Supply Chain Attacks,” *Proc. - IEEE Mil. Commun. Conf. MILCOM*, vol. 2021-November, pp. 458–463, 2021, doi: 10.1109/MILCOM52596.2021.9652901.

[5] N. Etemadi, Y. Borbon-Galvez, F. Strozzi, and T. Etemadi, “Supply chain disruption risk management with blockchain: A dynamic literature review,” *Inf.*, vol. 12, no. 2, pp. 1–25, 2021, doi: 10.3390/info12020070.

[6] T. Kieras, J. Farooq, and Q. Zhu, “I-SCRAM: A Framework for IoT Supply Chain Risk Analysis and Mitigation Decisions,” *IEEE Access*, vol. 9, pp. 29827–29840, 2021, doi: 10.1109/ACCESS.2021.3058338.

[7] I. Vasiliu-Feltes, M. Mylrea, C. Y. Zhang, T. C. Wood, and B. Thornley, “Impact of Blockchain-Digital Twin Technology on Precision Health, Pharmaceutical Industry, and Life Sciences: Conference Proceedings, Conv2X 2023,” *Blockchain Healthc. Today*, vol. 6, no. 2, 2023, doi: 10.30953/bhty.v6.281.

[8] Ujjwal Rao, “Overview of Cyber Security,” *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 47–51, 2023, doi: 10.48175/ijarsct-9470.

[9] M. M. Mijwil, O. J. Unogwu, Y. Filali, I. Bala, and H. Al-Shahwani, “Exploring the Top Five Evolving Threats in Cybersecurity: An In-Depth Overview,” *Mesopotamian J. CyberSecurity*, vol. 2023, pp. 57–63, 2023, doi: 10.58496/MJCS/2023/010.

[10] Motunrayo Oluremi Ibiyemi and David Olanrewaju Olutimehin, “Safeguarding supply chains from cyber-physical system attacks frameworks and strategies,” *Int. J. Manag. Entrep. Res.*, vol. 6, no. 6, pp. 2015–2023, 2024, doi: 10.51594/ijmer.v6i6.1240.

[11] J. Martínez and J. M. Durán, “Software supply chain attacks, a threat to global cybersecurity: SolarWinds’ case study,” *Int. J. Saf. Secur. Eng.*, vol. 11, no. 5, pp. 537–545, 2021, doi: 10.18280/IJSSE.110505.

[12] M. A. Serrano *et al.*, “Minimizing incident response time in real-world scenarios using quantum computing,” *Softw. Qual. J.*, vol. 32, no. 1, pp. 163–192, 2024, doi: 10.1007/s11219-023-09632-6.

[13] T. Wallis and P. Dorey, “Implementing Partnerships in Energy Supply Chain Cybersecurity Resilience,” *Energies*, vol. 16, no. 4, 2023, doi: 10.3390/en16041868.

[14] N. Krishnamoorthy and S. Umarani, “Implementation and management of cloud security for industry 4.O - data using hybrid elliptical curve cryptography,” *J. High Technol. Manag. Res.*, vol. 34, no. 2, 2023, doi: 10.1016/j.hitech.2023.100474.

[15] X. Masip-Bruin *et al.*, “Cybersecurity in ict supply chains: Key challenges and a relevant architecture,” *Sensors*, vol. 21, no. 18, 2021, doi: 10.3390/s21186057.

[16] H. Altaleb, F. Beatrix, F. Azemi, and R. Zoltan, “5G Evolution and Supply Chain Security in MENA Region: Challenges and Opportunities,” *2024 IEEE 22nd World Symp. Appl. Mach. Intell. Informatics, SAMI 2024 - Proc.*, pp. 149–156, 2024, doi: 10.1109/SAMI60510.2024.10432797.

[17] G. Segal, Y. Martsiano, A. Markinzon, A. Mayer, A. Halperin, and E. Zimlichman, “A blockchain-based computerized network infrastructure for the transparent, immutable calculation and dissemination of quantitative, measurable parameters of academic and medical research publications,” *Digit. Heal.*, vol. 9, 2023, doi: 10.1177/20552076231194851.

[18] N. Gupta, A. Tiwari, S. T. S. Bukkapatnam, and R. Karri, “Additive Manufacturing Cyber-Physical System: Supply Chain Cybersecurity and Risks,” *IEEE Access*, vol. 8, pp. 47322–47333, 2020, doi: 10.1109/ACCESS.2020.2978815.

[19] M. Ben Farah *et al.*, “A survey on blockchain technology in the maritime industry: Challenges and future perspectives,” *Futur. Gener. Comput. Syst.*, vol. 157, pp. 618–637, 2024, doi: 10.1016/j.future.2024.03.046.

[20] J. Mageto, “Big data analytics in sustainable supply chain management: A focus on manufacturing supply chains,” *Sustain.*, vol. 13, no. 13, 2021, doi: 10.3390/su13137101.

[21] T. Sawik, “Balancing cybersecurity in a supply chain under direct and indirect cyber risks,” *Int. J. Prod. Res.*, vol. 60, no. 2, pp. 766–782, 2022, doi: 10.1080/00207543.2021.1914356.

[22] A. Yeboah-Ofori and D. Opoku-Akyea, “Mitigating cyber supply chain risks in cyber physical systems organizational landscape,” *Proc. - 2019 Int. Conf. Cyber Secur. Internet Things, ICSIoT 2019*, pp. 74–81, 2019, doi: 10.1109/ICSIoT47925.2019.00020.

[23] Badis Hammi, Sherali Zeadally, and Jamel Nebhen, “Security threats, countermeasures, and challenges of digital supply chains,” *ACM Comput. Surv.*, 2023.

[24] M. Herburger, A. Wieland, and C. Hochstrasser, “Building supply chain resilience to cyber risks: a dynamic capabilities perspective,” *Supply Chain Manag.*, vol. 29, no. 7, pp. 28–50, 2024, doi: 10.1108/SCM-01-2023-0016.

[25] S. A. Asadollah, S. Imtiaz, A. Ghadim-Dehlaghi, M. Sjodin, and M. Sirjani, “Enhancing Cybersecurity through Comprehensive Investigation of Data Flow-Based Attack Scenarios,” *Jounral Cybersecurity Priv.*, vol. 4, no. 4, pp. 823–852, 2024, doi: https://doi.org/10.3390/jcp4040039.

[26] S. Al-Farsi, M. M. Rathore, and S. Bakiras, “Security of blockchain-based supply chain management systems: Challenges and opportunities,” *Appl. Sci.*, vol. 11, no. 12, 2021, doi: 10.3390/app11125585.

[27] T. Sawik, “A linear model for optimal cybersecurity investment in Industry 4.0 supply chains,” *Int. J. Prod. Res.*, vol. 60, no. 4, pp. 1368–1385, 2022, doi: 10.1080/00207543.2020.1856442.

[28] S. Al-Farsi, H. Bensmail, and S. Bakiras, “Securing Blockchain-Based Supply Chain Workflow against Internal and External Attacks,” *Machines*, vol. 10, no. 6, 2022, doi: 10.3390/machines10060431.

[29] Z. A. Collier and J. Sarkis, “The zero trust supply chain: Managing supply chain risk in the absence of trust,” *Int. J. Prod. Res.*, vol. 59, no. 11, pp. 3430–3445, 2021, doi: 10.1080/00207543.2021.1884311.

[30] J. Pérez-Morón, “Eleven years of cyberattacks on Chinese supply chains in an era of cyber warfare, a review and future research agenda,” *J. Asia Bus. Stud.*, vol. 16, no. 2, pp. 371–395, 2022, doi: 10.1108/JABS-11-2020-0444.

[31] D. N. Burrell *et al.*, “Supply chain and logistics management and an open door policy concerning cyber security introduction,” *Int. J. Manag. Sustain.*, vol. 9, no. 1, pp. 1–10, 2020, doi: 10.18488/journal.11.2020.91.1.10.

[32] C. Okafor, T. R. Schorlemmer, S. Torres-Arias, and J. C. Davis, “SoK: Analysis of Software Supply Chain Security by Establishing Secure Design Properties,” *SCORED 2022 - Proc. 2022 ACM Work. Softw. Supply Chain Offensive Res. Ecosyst. Defenses, co-located with CCS 2022*, pp. 15–24, 2022, doi: 10.1145/3560835.3564556.

[33] T. Sobb, B. Turnbull, and N. Moustafa, “Supply chain 4.0: A survey of cyber security challenges, solutions and future directions,” *Electron.*, vol. 9, no. 11, pp. 1–31, 2020, doi: 10.3390/electronics9111864.