Gradus Vol 11, No 3 (2024)
ISSN 2064-8014

GRADUS
GRADUS.KEFO.HU

MITIGATING CYBER RISKS IN INDUSTRIAL SUPPLY CHAIN: COMPREHENSIVE POLICY MODEL FOR INDUSTRY 4.0

*Fattah Abdul*0009-0000-3839-5085[*,1]

[1] *Doctoral School of Public Administration, University of Public Service, Hungary*

https://doi.org/10.47833/2024.3.ECO.011

Keywords:
Industry 4.0,
Industrial Supply Chain,
Cybersecurity,
Attack Simulation,
Policy Model

Article history:

Received	31 October 2024
Revised	20 November 2024
Accepted	25 November 2024

Abstract

This paper develops policy recommendations for improving cybersecurity in the manufacturing industry by exploring cyber vulnerabilities in industrial supply chains in Industry 4.0. The study uses data from previous cyberattacks and policy trends. It results from a case study on risk-handling simulation experiments to evaluate the potential impact of different industrial process related threats. The results highlight the increased risk and potential impact of cyber-attacks in industrial operations, data breaches, and physical damages in Industry 4.0. This study combines primary and secondary data from secondary sources along with system dynamics-based simulation experiments to develop comprehensive policy models that target mitigating cybersecurity vulnerabilities in industrial supply chains. The recommendations provide additional details on policy measures to (a) choose a centralized warehouse system to reduce cyber risk, (b) improve the resilience and security of Industry 4.0 systems in an environment where cyber threats continually evolve, technology advances come rapidly, and networks become increasingly interconnected

1 Introduction

The emergence of Industry 4.0 has revolutionized the industrial supply chain, leading to the rise of the cyber supply chain which is enhanced by cyber-based technologies to establish an effective value chain (Kshetri, 2022). The digital revolution integrates the cyber-physical system, the Internet of Things (IoT), and advanced analytics, resulting in a hyper-connected and data-rich environment. However, this digital shift exposes a significant volume of sensitive data related to products, inventory, manufacturing, and logistics to potential cybersecurity risks. Consequently, even minor security breaches in process technologies could be catastrophic (Kim & Im, 2014). Integrating IoT devices in production lines increases the vulnerability to cyber-attacks that could alter product characteristics or cause equipment damage (ibid).

The manufacturing industry has experienced a significant number of cyber-attacks in recent years, and in 2022, around a quarter of all detected cyber-attacks worldwide targeted the manufacturing sector (Statista, 2024d), a notable increase from previous years. These attacks have led to various consequences for manufacturing companies, with 65.2% experiencing disruptions to operations, 42.9% suffering damage to reputation, 29.5% facing unauthorized access, and 19.6% experiencing intellectual property theft (Statista, 2024e). The financial impact has also been

[*] Phone: +36302544522.
E-mail address: fattah.abdul@stud.uni-nke.hu

substantial, with major attacks like the one on Clorox in 2023 costing the company around $356 million due to declined sales and lower production volumes (ibid)

This study combines literature review, simulations, and policy modeling, distinguishing it from purely theoretical discussions. It followed a structured approach for reviews of the literature, with an iterative process that allows flexibility and refinement for search strategy and inclusion criteria as the research progresses. Based on exploratory research, this study analyzed both qualitative and quantitative data collected from secondary sources.

This study has applied the mixed method for data collection, consisting of a literature review and attack simulation-based experiments. This dual approach examines relevant studies on previous cyberattacks and assesses potential attacks by simulation data. The simulation experiments have been conducted to analyze the sensitivity of the supply chain in different mechanisms. The numerical data obtained in a research endeavor have been quantitatively examined using statistical operations.

Problem statement: The rise of Industry 4.0 poses a significant cybersecurity challenge for industrial supply chains. Human errors and increasing variations in attack types and defense mechanisms further increase the challenge. The study aims to address the vulnerabilities in the supply chain process in Industry 4,0 systems by utilizing a combination of historical attack analysis, current research efforts in attack simulation, and attack simulation data. The goal is to design a policy model that will effectively contribute to mitigating cybersecurity vulnerability and strengthen the overall security mechanisms of the industrial supply chain. The specific research question is - What are the most critical vulnerabilities in Industry 4.0 systems, and how can a combination of historical attack analysis, current research efforts, and attack simulation data be used to design comprehensive policy models for mitigating these vulnerabilities?

Research Objectives Investigating Major Cyberattacks and Vulnerabilities: To identify and categorize major cyber-attacks in the supply chain industry and analyze their economic and human impact. Impact Assessment: To assess the impact of major cyber security incidents on industrial processes. Analyzing Simulation Experiments: To figure out the policy mechanisms for improving industrial cybersecurity by assessing the attack simulation experiments. Policy Recommendation: To design policy models for the most effective strategies for mitigating supply chain attacks.

1.1 Literature Review

Industry 4.0 contributes to a significant shift in manufacturing, driven by Artificial Intelligence and automation. Unlike previous industrial revaluations, it appears to be more disruptive and has implications that go far beyond the limits of manufacturing plants (Schwab, 2017). Existing research on cyber risks in industrial supply chains is primarily focused on the growing importance of cyber risk management in supply chains (Ghadge et al., 2019; Ibiyemi & Olutimehin, 2024). Research in this area includes case studies on cyber-physical attacks, defense methods and frameworks, system modeling guides, as well as several surveys indicating the wider range of challenges and possibilities in securing modern production processes. Although there is some overlap between ICS and manufacturing cybersecurity needs, their distinct purpose led to different security approaches. The focus is now shifting to addressing vulnerabilities throughout the manufacturing enterprise through its supply chain. (de Souza Junior et al., 2021). Common risks include ransomware, phishing, and insider attacks, which exploit the complex interdependencies in supply chain networks (Ibiyemi & Olutimehin, 2024). To address these challenges, studies propose various strategies, including comprehensive cybersecurity frameworks, enhanced inter-organizational cooperation, and real-time threat detection systems (Ghadge et al., 2019; Ibiyemi & Olutimehin, 2024).

In addition, traditional automation-based, computer-controlled industrial manufacturing systems are gradually evolving into Smart Manufacturing Systems -SMSs (Tuptuk & Hailes, 2018). Smart manufacturing constructs dynamic, real-time optimized, and self-organizing value chains, which in turn require a corresponding legal framework like industry standards interfaces as well as harmonized company processes. One of the essential requirements is to provide details regarding a network architecture such as privacy, auto-configuration, and an easy use case (Hermann, et al., 2016). However, in this context of a digitized and highly connected environment, several challenges arise, among which is the issue of data security and production operations, given the high risk of attack on these systems, and their vulnerabilities, which are not yet fully known (Tuptuk & Hailes, 2018).

Existing literature emphasizes the need for a holistic, proactive approach to cybersecurity in supply chains, focusing on continuous improvement and adaptive strategies to protect against evolving threats (de Souza Junior et al., 2021). Although research has expanded to most areas related to Industry 4.0 risks, many gaps remain. Most studies have explored case studies of cyber-physical attacks, defensive frameworks, attack simulations using the MITRE framework, and modeling approaches. However, there is a pressing need for a policy framework that combines and addresses regulatory and technical requirements for Industry 4.0 (Vincent, R., 2015).

2 Methods

To understand the dynamics and security mechanisms for cyberattacks in industrial supply chains, the study employed a literature review of the literature in the field. Besides, the study simulated different configurations of the manufacturing supply chain process to assess the resilience of the industrial supply chain disruptions and profitability. The combination of theoretical and empirical analysis provides a policy model with recommendations to mitigate cyber risks in industrial supply chains. Data collection methods include both primary and secondary sources. Primary data was collected through the case study on risk pooling by simulation experiments and secondary data was collected from the literature review. The methodology is divided into two main components: (1) literature review and (2) simulation experiments.

Literature Review: The author identifies and analyzes existing studies on cyber vulnerabilities and attack simulations in industrial environments following a defined search protocol. This includes an extensive search through Scopus, IEEE, and Web of Science. This review focuses on publications post-2021 to understand more novel cyberattacks and policy mechanisms. Besides, statistical data on the impact of cyberattacks in the manufacturing industry and historical data on the events of major cyberattacks have been sourced from the Statista database.

Simulation Experiments: To assess the resilience of industrial supply chains, a case study of risk handling with risk pooling has been performed, where four simulation scenarios were experimented with using a system dynamics-based model. These experiments evaluated the impact of different configurations and disruptions across a global supply chain setup involving five factories and three suppliers. The key details of each experiment are as follows: 1. Baseline Simulation: The initial experiment created an idealized scenario with a single supplier and factory pair to establish optimal production capabilities and profit potential. 2. Supplier Downtime Impact: This simulation tested how extended downtime for a single supplier affects production and profitability, focusing on the buffer capacities within a single factory-supplier configuration. 3. Supply Chain Variability: Experiment three introduced variations in supplier downtime across multiple factories and suppliers, evaluating overall system stability and profitability under fluctuating supply conditions. 4. Centralized Warehouse and Risk Pooling: The final simulation applied a centralized warehouse model to consolidate resources and mitigate supply disruptions, assessing how risk pooling impacts profitability and resilience. Each simulation's quantitative outputs, such as profit margins, disruption impacts, and resource utilization, were statistically analyzed to derive insights into optimal configurations and vulnerabilities.

3 Results

3.1 Cyber Vulnerability and Regulatory Response

The manufacturing industry supply chain has been a particular vulnerability, with cybercriminals exploiting weaknesses in the interconnected network of suppliers and partners (Statista, 2024a). The SolarWinds attack in 2021, which impacted around 18,000 customers, is one of the most significant supply chain attacks in history (Statista, 2024b) Ransomware has been a common threat, hitting almost all manufacturing subsectors, with metal products and automotive productions being frequent targets (Statista, 2024d). The critical manufacturing sector was at high risk as well, representing approximately

35% of the reported security incidents to ICS-CERT in 2015 (ICS-CERT, 2016). The attacks aimed at obtaining unauthorized access to valuable info or business secrets, typically using well-researched phishing email scams like spear-phishing, again highlight the perpetual importance of cybersecurity actions within manufacturing. Cyber-physical attacks are one of the prime examples of how the systems that serve across all industry sectors and society can be vulnerable. That included, as shown in Table 1, a computer virus that damaged turbine control systems at a U.S. power company in the fall of 2012, causing an outage lasting three weeks.

Table 1. List of major industrial cyberattacks (compiled by author)

Attack Name	Type	Location	Cost (USD)
Clorox, 2003	Unknown, ransomware	North America	70m
Mondelez International, 2017	Encrypting malware	Chicago	100m
JBS, 2021	Ransomware	Australia and America	11m
Burnswick Co., 2022	Unknown	Global	85m
Applied Materials, 2023	Ransomware; Supply chain	United States	250m
Simpson Manufacturing Company, 2023	Ransomware(possible)	United States	Unknown
Toyota, 2022 & 2023	Ransomware	Global	Unknown
Bridgestone Americas, 2022	Ransomware, from LockBit	North and Latin America	Unknown

Similarly, an even more disastrous spear-phishing attack on a German steel mill in 2014 gave attackers the keys to the kingdom. It ultimately resulted in hackers gaining access to plant-level networks, which led to system failures and considerable physical destruction. In another case, a German nuclear plant was found infected with a computer virus in 2016, but it was not directly threatening. In 2016, a power grid in Ukraine was crippled by an attack that left over 100,000 people without power. In May 2017, production at a string of car manufacturing plants across Europe was halted due to the "WannaCry" ransomware virus. These incidents validate that loss-of-function attacks, also known as cyber-physical or destructive attacks, supposedly affect various types of targets, from production facilities to entire industries (Elhabashy, 2019)

In response to these risks, the European Commission (COM) adopted "Proposal for a Directive on measures to achieve a high common level of cybersecurity across the Union: NIS 2)". The European Data Protection Supervisor (EDPS) submits specific recommendations aimed at aligning the proposal text with existing data protection rules and providing further clarity regarding the terminology used in the proposed Quarters Regulation. Article 83 of GDPR lists the fines for breaches in data security and classifies them into two tiers depending upon the seriousness. Smaller offenses, such as administering incorrect or late notifications of a breach, can result in fines up to 10 million (or 2% of the company value annually), and for larger breaches up to 20 million specifically with risk-4 percentage points added on top. In a bid to make cybersecurity part of the manufacturing industry, the EU harmonization legislation will come into effect soon, which means manufacturers need to design their products focusing on cyber protection. Although the current safety standards specify what needs to be done, they do not provide guidelines for implementation.

3.2 Insights from Simulation Experiment

Four experiments are conducted in this study to evaluate the performance and resilience of a five-factory, three-supplier global supply chain under varied simulation configurations. *Experiment 1:* The first experiment was aimed at establishing an ideal condition (i.e., one supplier and one factory) to determine the theoretical capabilities and profitability of the system. The experiment results in all five factories showed that the system is running at full capacity, meeting supplier demand smoothly. The system gained a profit of 200,468 financial Units (the upper limit of how much it could support) in its best-case results, showing unimpaired performance. Stock levels were effectively managed for the warehouses to ensure a balanced production.

The *Experiment 2* simulations evaluated the effects of supplier downtime on production and profit, focusing here, however, on a single factory-supplier pair (European factory -Supplier). Results found that the line was able to handle suppliers' downtime for up to 5 hours without losing any production. After this point, production and profits experienced a sharp fall downward due to the lack of warehouse capacity to act as buffer stock during supplier disruption. We can live with short-term outages, but extended downtime was a considerable threat to the bottom line. Experiment Configuration Maximum Profit Average Profit Supplier Disruptions Warehouse Efficiency

Table 2. Key findings of the experiments(prepared by author)

Experiment	Configuration	Supplier Disruptions	Warehouse Efficiency
Experiment 1	Single supplier, single factory	No disruptions	Efficient
Experiment 2	Single supplier-factory pair (Europe)	Up to 5 hours downtime manageable	Buffer against short outages
Experiment 3	Three suppliers, five factories	Significant impact (10% production loss)	Vulnerable to disruptions
Experiment 4	Centralized warehouse	Reduced sensitivity	Risk-pooling strategy

Experiment 3 focused on the potential impact of additional variability within the whole supply chain system consisting of 5 manufacturing factories and three suppliers (for different possible settings and combinations of downtime for suppliers). This finds that the program was a loser overall, with an average profit across all simulations of 183,164 financial units (a -10% relative loss to ideal). Profit responses to supplier outages were highly variable between individual runs, with the bulk of scenarios including some profit loss mitigated across suppliers. Very few runs and the exact right profit could have been obtained, thus making ISO a fragile system of extremely low risk but needing an infinitely more robust approach. In *Experiment 4*, unlike the above two mechanisms being tested as independent solutions at the same time, we evaluated a centralized warehouse serving all factories and implemented a risk-pooling strategy to mitigate production uncertainties. With this optimized layout, the average profit is increased to 202646 financial units - a result that eventually overcomes any theoretical maximum value of the original configuration. There was evidence of more stable, improved performance in the profit distribution, and smaller total supply chains were less sensitive to individual supplier disruption when storage became centralized.

These experiments illustrate three powerful lessons for supply chain management. Although optimal performance is only possible when the world's largest nearshore supplier system operates in pristine conditions, just a few moments of down-supply time can add up to huge losses for production and profit. Effect of Disruption on Supply The whole supply chain is just a single point away from disruptions, and mostly, it results in profits and losses.

Overall, this experiment showed that risk-pooling via centralization is highly recommended in enhancing supply chain resilience and profitability, where risks can be effectively pooled while resource allocation may benefit from collective optimization. Thus, a more robust approach when managing disruptions. This study helps firms recognize the strategic aspect of inventory management; diversification options in suppliers and locating storage spaces centrally can only add more resilience to the supply chain.

4 Discussion

4.1 Policy Recommendation

The case study offers an understanding of risk-pooling and supply chain coordination to cope with disruptions due to IT-induced problems. Some policy insights for industries that want to build resilience and profitability based on risk pooling case studies and literature review findings include:

Table 3. Policy Model for Cyber Resilience in Industry(prepared by author)

Policy	Justification	Implementation
Centralized Warehouse System	Improves efficiency, reduces supplier disruptions	invest in a central warehouse facility and optimize logistics
Robust Inventory Management	Buffers against short-term supply chain disruptions	Implement advanced inventory tracking systems
Diversified Supplier Base	Minimizes reliance on single source suppliers	relationships with multiple reliable suppliers
Regular Risk Assessment and Simulation	Proactively identifies and addresses potential vulnerabilities	Conduct regular risk assessments and simulations, and develop contingency plans
Enhanced IT Security Infrastructure	Protects against cyberattacks and IT-induced disruptions	Invest in firewalls, intrusion detection systems, and training
Adherence to Cybersecurity Regulations	Mitigates legal risks and enhances security posture	ensure legal compliance
Collaborative Relationships with Suppliers	Facilitates rapid response to disruptions	Establish communication and collaboration with suppliers
Supply Chain Automation	Improves visibility, efficiency, and predictive analytics	Invest in technologies like IoT, AI, and machine learning
Harmonized Regulatory Framework	Ensures consistent standards and practices	Advocate for a unified regulatory framework

Centralized warehouse: Instead of a decentralized supply process, a direct connection to the individual factories by using a centralized warehouse system is highly critical for enhanced efficiency. Justification: Simulation results (Experiment 4) showed that a central warehouse is more stable and generates more average profit. In this case, even if one or two suppliers fail in the process, the industry will still be able to manage the risk posed by it.

Robust Inventory Management: to protect against supplier downtime, keeping a robust track of inventory in the warehouses is recommended to reduce risks. Justification: Test 2 reveals that inventory levels can ensure the production process without interruption for up to the duration of a 5-hour supplier outage. Inventory allows for absorbing short-term disruptions without stopping the production processes.

Diversification of Suppliers: Increase the number of supplies and remove single-source dependency on critical parts. Justification: Experiment 3 demonstrated that the system’s vulnerability to supplier outages can have a substantial impact on profitability. The risk of a catastrophic supply failure by one supplier is significantly higher. At the same time, sourcing from diverse vendors can reduce such risks.

Regular Risk Assessment and Simulation: Regular assessment of vulnerabilities, risks, and simulated attacks on the company supply chain can help prepare for and mitigate sudden disruptions. Justification: The simulations in this study are very useful data for understanding the influence of various disruption lengths and combinations. Frequent evaluations can allow us to adopt strategies in real-time, making the proper decisions at every critical juncture.

Enhanced IT Security Infrastructure: Companies needed to allocate more budgets for modern cybersecurity mechanisms to reduce the chance of cyber-attacks causing disruptions in the process. Justification: IT problems are classified as high-severity production incidents. To avoid such breakdowns, it is recommended to improve IT infrastructure in companies.

Implementation of Regulations: It is imperative to strictly execute EU/USA regulations on cybersecurity to reduce vulnerability: Justification: The study found that non-compliance with the GDPR and Cybersecurity regulations is a major cause of cyberattacks in different manufacturing industries worldwide. Therefore, strict execution of that regulation is highly recommended, not only for the security of the supply chain process but also for legal consequences.

Security Collaboration with Suppliers: Keeping in touch with suppliers more directly to be able to respond and react faster during disruption situations. Justification: Collaboration makes the supply chain more resilient and less vulnerable to sudden disruption in the process. The experiments also suggest that suppliers and manufacturers need to collaborate to develop backup plans so they can respond more quickly when things go wrong.

Automation of supply chain: Investment in technology infrastructure investment to enhance visibility and automation into the supply chain. Justification: By modernizing technologies, there could be a lot of advancements made, such as real-time data and predictions for eliminating risks before any influence causes production.

Harmonized regulatory mechanism: The regulatory mechanism needs to address the overall cybersecurity measures in the manufacturing industry, specifically the supply chain. Justification: The manufacturing industry is found to be the most vulnerable to attacks, experiencing the highest number of attacks in recent years. However, there are no harmonized regulations implemented, even though adopted, by the European Union that address this cause. By implementing these policy recommendations, companies can significantly enhance their supply chain resilience, reduce the impact of IT-related disruptions, and maintain higher profitability even in the face of unexpected challenges.

5 Conclusion

In this age of Industry 4.0, a robust and complex mechanism for enhanced cybersecurity is critical for maintaining modern production processes. Human error is the biggest cybersecurity threat, accounting for over 80% of the incidents. Industries can significantly reduce the risk by selecting a risk-pooling strategy in the supply chain process. Policy recommendations like a centralized warehouse, diversification of supplies, and regular risk assessments need to be prioritized for companies to improve their supply chain resilience against cyber threats. Besides, companies increase collaboration among supplies in a diverse range of matters, from security to process automation. Additionally, regulatory mechanisms also need to be executed properly to avoid the risk of cyber-attacks and fines. Moving forward, continuous investment in advanced IT security and automation technologies, along with real-time data analysis and predictive capabilities, will be essential in helping industries anticipate and prevent cyber threats before they cause major issues. By embracing these technological advancements and promoting a culture of cybersecurity awareness, industries can successfully navigate the evolving threat landscape of Industry 4.0, ensuring a secure and thriving future for manufacturing.

Acknowledgment

I acknowledge Zsolt Molnar for conducting the Risk Pooling case study as part of the TKP, which significantly contributed to this research.

TKP2021-NKTA-51 has been implemented with the support provided by the Ministry of Culture and Innovation of Hungary from the National Research, Development and Innovation Fund, financed under the TKP2021-NKTA funding scheme.

Reference

[1] de Souza Junior, A. A., de Souza Pio, J. L., Fonseca, J. C., de Oliveira, M. A., de Paiva Valadares, O. C., & da Silva, P. H. S. (2021). The state of cybersecurity in smart manufacturing systems: A systematic review. *European Journal of Business and Management Research, 6*(6), 188–194.

[2] Elhabashy, A. (2019). Machine learning techniques for detecting cyber-physical attacks on manufacturing systems. In *2019 IEEE International Conference on Electro Information Technology (EIT)* (pp. 869–875). IEEE. https://ieeexplore.ieee.org/document/8900358

[3] Elhabashy, A. E., Wells, L. J., & Camelio, J. A. (2019). Cyber-physical security research efforts in manufacturing—a literature review. *Procedia Manufacturing, 34*, 921–931. http://dx.doi.org/10.1080/00207543.2019.1629670

[4] Ghadge, A., Wurtmann, H., & Seuring, S. (2019). Managing climate change risks in global supply chains: A review and research agenda. *International Journal of Production Research, 58*(1), 44–64.

[5] Hermann, M., Pentek, T., & Otto, B. (2016, January). Design principles for industrie 4.0 scenarios. In *2016 49th Hawaii international conference on system sciences (HICSS)* (pp. 3928-3937). IEEE.

[6] Hacks, S., Butun, I., Lagerström, R., Buhaiu, A., Georgiadou, A., & Michalitsi Psarrou, A. (2021, August 17). Integrating security behavior into attack simulations. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3465481.3470475

[7] Huraj, L., Horak, T., Strelec, P., & Tanuska, P. (2021). Mitigation against DDoS attacks on an IoT-based production line using machine learning. *Applied Sciences, 11*(4), 1847. https://www.mdpi.com/2076-3417/11/4/1847

[8] Ibiyemi, M. O., & Olutimehin, D. O. (2024). Cybersecurity in supply chains: Addressing emerging threats with strategic measures. *International Journal of Management & Entrepreneurship Research, 6*(6).

[9] ICS-CERT. (2016). ICS-CERT Monitor Newsletters: November-December 2015.

[10] Kagermann, H., Lukas, W. D., & Wahlster, W. (2013). Recommendations for implementing the strategic initiative INDUSTRIE 4.0: Securing the future of the German manufacturing industry; final report of the Industrie 4.0 Working Group. *Forschungsunion*.

[11] Kim, K. C., & Im, I. (2014). Issues of cyber supply chain security in Korea. *Technovation, 34*(7), 387–388. https://doi.org/10.1016/J.TECHNOVATION.2014.01.003

[12] Kshetri, N. (2022). Economics of supply chain cyberattacks. *IT Professional, 24*(3), 96–100. https://doi.org/10.1109/MITP.2022.3172877

[13] Kusiak, A. (2017). Smart manufacturing. *International Journal of Production Research, 56*(1–2), 508–517.

[14] Mittal, S., Khan, M. A., Romero, D., & Wuest, T. (2019). Smart manufacturing: Characteristics, technologies, and enabling factors. *Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture, 233*(5), 1342–1361.

[15] National Institute of Standards and Technology (NIST). (2017). As cited in Kusiak, A. (2017).

[16] Rajesh, P., Alam, M., Tahernezhadi, M., Monika, A., & Chanakya, G. (2022). Analysis of cyber threat detection and emulation using MITRE attack framework. *2022 International Conference on Intelligent Data Science Technologies and Applications (IDSTA)*, 4–12. https://doi.org/10.1109/IDSTA55301.2022.9923170

[17] Schwab, K. (2017). *The fourth industrial revolution*. Currency.

[18] Statista. (2024a). Cybercrime and the manufacturing industry worldwide. Retrieved from https://www.statista.com/study/134808/cyber-crime-in-the-manufacturing-industry-worldwide/

[19] Statista. (2024b). Global threat groups targeting industry sectors. Retrieved from https://www.statista.com/statistics/1373900/global-threat-target-industries/

[20] Statista. (2024c). Manufacturing cyberattacks worldwide. Retrieved from https://www.statista.com/statistics/1374061/cyber-attacks-manufacturing-share-worldwide/

[21] Statista. (2024d). Cyberattack distribution 2023, by type. Retrieved from https://www.statista.com/statistics/1382266/cyber-attacks-worldwide-by-type/

[22] Statista. (2024e). Top manufacturing cyberattacks costs 2024. Retrieved from https://www.statista.com/statistics/1374779/manufacturing-attacks-worldwide-cost/

[23] Toker, A., Smith, B., & Johnson, C. (2021). Enhancing cybersecurity resilience in critical infrastructure: A case study of ICS security in a drinking water system using MITRE frameworks. *International Journal of Critical Infrastructure Protection, 14*, 100312.

[24] Tuptuk, N., & Hailes, S. (2018). Security of smart manufacturing systems. *Journal of Manufacturing Systems, 47*, 93–106.

[25] Vincent, R. (2015). Side-channel attack detection in cyber-physical systems using machine learning. *arXiv preprint*. Retrieved from https://arxiv.org/abs/1505.06955

[26] Weippl, E. R. (2017). Information security in cyber-physical production systems: Challenges and solutions. *Procedia Manufacturing, 13*, 1212–1219. https://www.sciencedirect.com/science/article/pii/S2351978917302321

[27] Xiong, W., Legrand, E., Åberg, O., & Lagerström, R. (2022). Cybersecurity threat modeling based on the MITRE enterprise ATT&CK matrix. *Software and Systems Modeling, 21*(1), 157–177. https://doi.org/10.1007/s10270-021-00898-7