International Journal of Academic Management Science Research (IJAMSR)
ISSN: 2643-900X
Vol. 9 Issue 4 April - 2025, Pages: 461-466

Cybersecurity Threats in Logistics and Shipping: Mitigation Strategies for Supply Chain Resilience

Julius Olatunde Omisola[1], Emmanuel Augustine Etukudoh [2], Ekene Cynthia Onukwulu[3] and Grace Omotunde Osho[4]

[1]Platform Petroleum Limited, Nigeria.
[2]ASCA- Ringadas Limited, Nigeria.
[3]Independent Researcher, Lagos, Nigeria
[4]Guinness Nigeria,Plc.

Corresponding Editor: cynthia.onukwulu@gmail.com

Abstract: *This paper explores the critical role of cybersecurity in maintaining the resilience of the logistics and shipping industry's supply chain. In an era of digital connectivity and interdependence, the sector faces evolving cybersecurity threats that can lead to data breaches, ransomware attacks, and disruptions in operations. The paper outlines various cybersecurity threats, including unauthorized access, phishing, IoT vulnerabilities, and supply chain interdependencies. To address these challenges, a comprehensive set of mitigation strategies is presented, encompassing employee training, access controls, regular audits, secure partnerships, incident response planning, and continuous monitoring. The effectiveness of these strategies is illustrated through real-world case studies, emphasizing the importance of proactive cybersecurity measures for sustained supply chain resilience in the face of evolving threats. The insights provided aim to guide industry stakeholders and decision-makers in fortifying their cybersecurity defenses and ensuring the uninterrupted flow of goods and services within the logistics and shipping ecosystem.*

Keywords: Cybersecurity, Threats, Logistics, Shipping, Mitigation, Strategies, Supply Chain, Resilience.

1.0 INTRODUCTION

The logistics and shipping industry serves as the backbone of global trade, facilitating the movement of goods across vast supply chains and connecting manufacturers, suppliers, and consumers worldwide (Tien et al., 2019). This multifaceted industry encompasses various modes of transportation, including shipping, air freight, rail, and trucking, as well as a complex network of warehouses, distribution centers, and ports. The efficiency and effectiveness of this intricate system play a pivotal role in the timely delivery of products, ultimately impacting economies and consumer satisfaction (Heikkilä, 2002). Logistics and shipping involve the coordination and synchronization of numerous processes, from procurement and production to transportation and distribution (Tseng et al., 2005). Companies operating in this sector constantly strive to optimize their supply chains to reduce costs, enhance speed, and adapt to dynamic market demands. As the industry embraces technological advancements such as automation, real-time tracking, and data analytics, the reliance on interconnected digital systems becomes increasingly integral to its functioning. The logistics sector, however, is not immune to challenges. It faces complexities arising from regulatory compliance, fluctuating market conditions, geopolitical uncertainties, and, notably, evolving cybersecurity threats (Luo, 2022). As technology becomes more deeply ingrained in supply chain operations, the industry is exposed to cyber risks that can disrupt the seamless flow of goods, compromise sensitive information, and jeopardize the reliability of the entire logistics and shipping ecosystem (Allioui and Mourdi, 2023).

Cybersecurity has emerged as a paramount concern for the logistics and shipping industry due to the escalating frequency and sophistication of cyber threats (Okoli et al., 2024). The digital transformation that has enhanced efficiency and connectivity within supply chains also brings with it vulnerabilities that malicious actors can exploit (Yeboah-Ofori et al., 2021). The consequences of cybersecurity breaches extend beyond financial losses; they encompass operational disruptions, reputational damage, and potential legal ramifications (Adewusi et al., 2024). Maintaining supply chain resilience is contingent upon the industry's ability to safeguard critical data, digital assets, and interconnected systems from cyber threats (Patel, 2023). A breach in cybersecurity not only poses a direct threat to the confidentiality, integrity, and availability of information but also has the potential to cascade through the entire supply chain, affecting partners, vendors, and customers. In a hyper-connected world, where data is exchanged seamlessly across borders and between stakeholders, the need for robust cybersecurity measures cannot be overstated (Serôdio et al., 2023). As logistics and shipping companies adopt digital technologies, including Internet of Things (IoT) devices, cloud computing, and autonomous systems, the attack surface widens, requiring a proactive and comprehensive approach to cybersecurity (Makhdoom et al., 2018). In light of these challenges, this paper aims to delve into the specific cybersecurity threats faced by the logistics and shipping industry and elucidate effective mitigation strategies. By understanding the intersection of cybersecurity and supply chain resilience, stakeholders can fortify their defenses, ensuring the continued efficiency, reliability, and security of the global logistics and shipping ecosystem.

2.1 CYBERSECURITY THREATS IN LOGISTICS AND SHIPPING

The logistics and shipping industry, being highly reliant on digital technologies, faces a myriad of cybersecurity threats that can compromise the integrity and confidentiality of sensitive information (Das and Mukherjee, 2024). Data breaches and theft, in particular, present significant challenges, encompassing, Unauthorized access to sensitive information remains a critical cybersecurity threat in the logistics and shipping sector. With the increasing digitization of operational processes and the adoption of cloud-based systems, the risk of unauthorized access rises substantially (Yathiraju, 2022). Malicious actors may exploit vulnerabilities in software, weak authentication mechanisms, or gaps in network security to gain entry into critical systems (Perwej et al., 2021). The consequences of unauthorized access are profound, as it can lead to the compromise of shipment details, inventory information, and operational plans. The unauthorized retrieval of such sensitive data not only threatens the proprietary information of logistics companies but also has the potential to disrupt the flow of goods and compromise the integrity of the entire supply chain (Atadoga et al., 2024). The exchange of information with customers, suppliers, and other partners is integral to the logistics and shipping ecosystem. The theft of customer and supplier data represents a significant cybersecurity risk, as this information is not only valuable to the organization but also crucial for maintaining trust and compliance with regulatory standards (Abidin et al., 2019). Cybercriminals may target customer databases, supplier contracts, and payment information for financial gain or to gain a competitive advantage. The theft of such data not only has financial implications but also jeopardizes the reputation of the company, potentially leading to legal consequences and loss of business relationships. To mitigate these risks, logistics and shipping companies need to implement robust cybersecurity measures such as encryption, secure access controls, and regular security audits (Sobb et al., 2020). Additionally, educating employees about the importance of cybersecurity and implementing stringent authentication protocols can contribute to a more resilient defense against unauthorized access and data theft.

Ransomware attacks have become a pervasive and disruptive threat to the logistics and shipping industry, impacting operations and imposing financial burdens on organizations (Snyder, 2022). Ransomware attacks involve the malicious encryption of critical systems and data, rendering them inaccessible until a ransom is paid. In the logistics and shipping context, this could result in the disruption of key operational systems, affecting shipment tracking, inventory management, and communication channels. The encryption of critical systems can lead to operational downtime, delayed deliveries, and potential financial losses. The interconnected nature of logistics operations amplifies the impact, as disruptions in one area can have cascading effects across the entire supply chain (Li et al., 2021). The financial implications of ransomware attacks extend beyond the immediate operational disruptions. Companies faced with a ransomware incident must grapple with the decision of whether to pay the ransom to regain access to their systems (Leo et al., 2022). While paying the ransom may expedite the restoration of operations, it comes with ethical, legal, and financial considerations. Ransom payments do not guarantee the complete recovery of data, and they may encourage further attacks (Brewer, 2016). Additionally, organizations must weigh the potential reputational damage associated with succumbing to extortion. As such, developing robust backup and recovery mechanisms, alongside proactive cybersecurity measures, is essential to mitigate the risks posed by ransomware attacks.

Phishing and social engineering attacks are prevalent tactics used by cybercriminals to exploit human vulnerabilities within the logistics and shipping industry (Cihat, 2023). Phishing attacks typically involve the use of deceptive emails, messages, or websites to manipulate employees into disclosing sensitive information such as login credentials or financial details. In the logistics sector, where employees often interact with a variety of digital platforms and communication channels, the risk of falling victim to phishing attempts is heightened. Successful phishing attacks can lead to unauthorized access, data breaches, and even compromise critical systems (Gupta et al., 2017). Training employees to recognize and report phishing attempts is crucial for building a resilient defense against these social engineering tactics. Beyond data theft, phishing attacks can serve as a vector for spreading malware within logistics and shipping networks. Malicious attachments or links in phishing emails may deliver malware payloads that can compromise the integrity of systems, disrupt operations, or serve as a gateway for more advanced cyber threats (Sullivan, 2005). Implementing robust email filtering, conducting regular employee training, and fostering a culture of cybersecurity awareness are essential strategies to mitigate the risks associated with phishing and social engineering attacks. The proliferation of Internet of Things (IoT) devices in the logistics and shipping industry introduces new cybersecurity challenges (Djenna et al., 2021). The integration of IoT devices, such as sensors, RFID tags, and connected vehicles, enhances visibility and efficiency within the supply chain. However, insecure IoT devices pose a significant risk, as they may serve as entry points for cybercriminals to infiltrate the network. Compromised IoT devices can be exploited to manipulate tracking information, tamper with shipment data, or disrupt the functionality of interconnected systems (Makhdoom et al., 2018). Strengthening the security of IoT devices through regular updates, robust authentication mechanisms, and adherence to industry standards is crucial for mitigating these vulnerabilities. The reliance on IoT devices for real-time tracking and monitoring of shipments makes logistics and shipping operations more susceptible to disruptions. Cyberattacks targeting IoT devices can result in inaccurate tracking information, delays in transportation, and potential loss or theft of cargo (Stellios et al., 2018). To address these vulnerabilities, logistics companies should implement comprehensive security protocols for IoT devices, conduct regular security assessments, and collaborate with suppliers to ensure the deployment of secure and up-to-date IoT technologies.

The interconnected nature of supply chains introduces cybersecurity risks stemming from interdependencies between different entities. The modern supply chain relies on a network of third-party vendors and service providers. Cyberattacks on these external entities can have a direct impact on the security and functionality of the entire supply chain (Pandey et al., 2020). This includes disruptions to logistics services, data breaches, or the compromise of critical infrastructure shared among multiple stakeholders. Collaborating with third-party vendors to establish and enforce stringent cybersecurity standards, conducting regular audits, and requiring transparency in their security practices are crucial steps in mitigating these supply chain interdependencies. A cyber incident affecting one part of the supply chain can have cascading effects on interconnected systems. For example, a disruption in inventory management systems may lead to delays in production, transportation, and distribution. The ripple effect of such disruptions can result in financial losses, reputational damage, and strained relationships with customers and partners (Blom and Niemann, 2022). To enhance resilience against supply chain interdependencies, organizations should implement contingency plans, diversify suppliers where feasible, and establish clear communication channels for rapid response in the event of a cybersecurity incident affecting any part of the supply chain. The logistics and shipping industry faces a complex and evolving landscape of cybersecurity threats that require multifaceted strategies for mitigation. By addressing data breaches and theft, ransomware attacks, phishing and social engineering, IoT vulnerabilities, and supply chain interdependencies, organizations can fortify their cybersecurity defenses and enhance the overall resilience of the supply chain (An, 2022). Proactive measures, including employee training, technological safeguards, and collaboration across the supply chain, are essential in navigating the challenges posed by cybersecurity threats in this dynamic and interconnected industry.

2.2 MITIGATION STRATEGIES FOR CYBERSECURITY THREATS

The dynamic and interconnected nature of the logistics and shipping industry demands a proactive approach to cybersecurity (Andrea, 2017). To fortify defenses against the diverse range of cyber threats, organizations should implement comprehensive mitigation strategies. Instituting regular cybersecurity training programs is crucial to keep employees informed about evolving cyber threats, best practices, and company-specific security policies (Abrahams et al., 2024). Training sessions should cover topics such as identifying phishing attempts, recognizing social engineering tactics, secure password management, and the importance of reporting suspicious activities promptly (Campbell, 2019). Given the prevalence of phishing attacks, organizations should conduct targeted awareness campaigns to educate employees about the dangers of phishing. Simulated phishing exercises can help employees recognize and respond effectively to phishing attempts, fostering a culture of heightened cybersecurity awareness.

Robust Access Controls and Authentication, enforcing multi-factor authentication adds an additional layer of security, requiring users to verify their identity through multiple authentication methods (Kaiser et al., 2021). MFA reduces the risk of unauthorized access even if login credentials are compromised, enhancing overall access security. Implementing the principle of least privilege ensures that employees have access only to the information necessary for their specific roles. Regularly reviewing and updating access permissions based on job roles minimizes the potential impact of insider threats and limits the attack surface (Plachkinova and Knapp, 2023).

Regular Cybersecurity Audits and Assessments, regular vulnerability assessments and penetration testing help identify and address weaknesses in the organization's cybersecurity infrastructure. These assessments simulate real-world cyber threats, allowing organizations to proactively mitigate vulnerabilities before they can be exploited. Analyzing the results of cybersecurity audits enables organizations to identify and address vulnerabilities in their systems and networks (Bozkus Kahyaoglu and Caliyurt, 2018). Swift remediation of weaknesses ensures a robust cybersecurity posture and reduces the likelihood of successful cyberattacks.

Secure Supply Chain Partnerships, prioritizing cybersecurity when selecting and evaluating third-party vendors is essential to ensure that they adhere to similar security standards (Keskin et al., 2021). Regular assessments of vendor cybersecurity practices, including their data protection measures and incident response capabilities, help mitigate supply chain risks. Establishing clear contractual agreements that outline cybersecurity standards and expectations is vital for holding third-party vendors accountable. These agreements may include requirements for regular security audits, compliance with industry standards, and incident response protocols (Peltier, 2016).

Incident Response and Recovery Planning, creating well-defined incident response plans tailored to the logistics and shipping industry enables organizations to respond effectively to cybersecurity incidents (Lekota and Coetzee, 2019). Regularly testing these plans through simulated exercises ensures that the response team is prepared to mitigate and recover from various cyber threats. Clear communication protocols are essential to coordinate the response efforts during a cyber incident (Skopik et al., 2016). Establishing communication channels with internal teams, external partners, regulatory authorities, and customers helps maintain transparency and facilitates a swift response (Azapagic, 2003).

Real-time monitoring of network activities allows organizations to detect and respond promptly to suspicious behavior or anomalies (Goodall et al., 2018). Intrusion detection systems, log analysis, and network traffic monitoring contribute to the early identification of potential cyber threats. Continuous monitoring of threat intelligence sources keeps organizations abreast of the latest cyber threats and attack vectors. This information enables proactive adjustments to cybersecurity strategies and the implementation of targeted defenses against emerging threats (Saini and Saini, 2007). The successful mitigation of cybersecurity threats in the logistics and shipping industry requires a holistic and proactive approach. By investing in employee training, robust access controls, regular cybersecurity audits, secure supply chain partnerships, incident response planning, and continuous monitoring with threat intelligence, organizations can significantly enhance their cybersecurity resilience and safeguard the integrity of their operations in an ever-evolving threat landscape (Mughal, 2018).

2.3 CASE STUDIES

Maersk Cyberattack (2017), in 2017, Maersk, one of the world's largest shipping companies, fell victim to the NotPetya ransomware attack. The malware spread rapidly through the company's global network, encrypting critical systems and data. The attack had a cascading effect, disrupting Maersk's operations worldwide. The company's ability to handle bookings, manage container loadings, and track shipments was severely impaired. The financial impact of the incident was substantial, with estimated losses exceeding $300 million.

Cosco Shipping Cyber Incident (2018), in 2018, Chinese shipping giant Cosco suffered a cyber incident that impacted its operations in the United States. The company's communication systems were disrupted, leading to issues with customer service and terminal operations. While the incident did not result in a significant data breach, it highlighted the vulnerability of global shipping operations to cyber threats. Cosco had to temporarily revert to manual processes to manage its operations during the recovery period.

CMA CGM Cyberattack (2020), french shipping giant CMA CGM experienced a cyberattack in 2020 that led to a temporary disruption in its online services. The attack affected the company's booking platform, causing delays in customer transactions. Although the incident did not result in a significant operational impact, it underscored the persistent threat landscape faced by the logistics and shipping industry.

Analyzing Successful Mitigation Strategies Employed by Organizations, Maersk's Response and Recovery (2017), Maersk's swift response involved isolating infected systems to prevent the spread of the ransomware further. The company maintained transparent communication with customers, partners, and the public, keeping stakeholders informed about the situation and recovery efforts. Maersk's ability to restore operations relied on robust backup systems, allowing them to recover data without succumbing to ransom demands.

Cosco's Incident Management (2018), Cosco's decision to revert to manual operations during the incident showcased the importance of having contingency plans in place for times when digital systems are compromised. Enhanced Cybersecurity Measures:* Following the incident, Cosco implemented enhanced cybersecurity measures, including network segmentation and improved incident response protocols, to bolster its defenses against future cyber threats.

CMA CGM's Resilience (2020), CMA CGM demonstrated resilience by swiftly recovering from the cyberattack and restoring normal operations. The incident prompted the company to reevaluate and strengthen its cybersecurity measures, including employee training, network monitoring, and system updates, to mitigate the risk of similar incidents in the future. Successful mitigation strategies include rapid incident response, transparent communication, robust backup and recovery plans, and ongoing improvements to cybersecurity protocols. Organizations that proactively invest in cybersecurity resilience are better positioned to navigate the complex and evolving landscape of cyber threats within the logistics sector (Safitra et al., 2023).

2.4 CONCLUSION

The logistics and shipping industry operates at the intersection of global trade, technological advancement, and intricate supply chain networks. In navigating this complex landscape, the industry faces a range of cybersecurity threats that can compromise the integrity, confidentiality, and availability of critical data and systems. The challenges posed by cybersecurity threats in logistics and shipping underscore the critical need for proactive measures to enhance supply chain resilience. As the industry continues to embrace digital technologies, interconnected systems, and global collaboration, the following key considerations emphasize the importance of proactive cybersecurity measures, Proactive cybersecurity measures help identify and mitigate risks before they escalate, ensuring that the industry remains adaptable to evolving threats. Continuous risk assessment and monitoring enable organizations to stay ahead of emerging cybersecurity challenges and swiftly adapt their defenses. Supply chain resilience relies on operational continuity, and proactive cybersecurity measures contribute to minimizing disruptions. Planning for and mitigating cyber threats in advance ensures that operations can continue seamlessly, even in the face of potential cyber incidents. The logistics and shipping industry thrives on trust and reputation. Proactive cybersecurity measures protect customer data, build trust, and safeguard the reputation of organizations within the supply chain. Demonstrating a commitment to cybersecurity resilience enhances customer confidence and reinforces the industry's reputation as a reliable and secure partner in global trade. Proactive cybersecurity measures align with regulatory requirements and industry standards, reducing the risk of legal and regulatory consequences. Compliance with cybersecurity standards helps organizations demonstrate due diligence in protecting sensitive information and maintaining the integrity of the supply chain. Proactive cybersecurity measures foster a culture of collaboration and information sharing within the industry. Sharing threat intelligence, best practices, and lessons learned enhances the collective cybersecurity posture of the logistics and shipping community, creating a united front against cyber threats. The logistics and shipping industry must recognize cybersecurity as an integral component of supply chain resilience. By proactively addressing and mitigating key cybersecurity threats through continuous improvement, collaboration, and a commitment to best practices, organizations can fortify their defenses and ensure the enduring reliability, security, and efficiency of global logistics operations. As the industry evolves, so too must its cybersecurity measures to meet the challenges of an ever-changing digital landscape.

REFERENCES

1. Abidin, M. A. Z., Nawawi, A., & Salin, A. S. A. P. (2019). Customer data security and theft: a Malaysian organization’s experience. *Information & Computer Security*, *27*(1), 81-100.
2. Abrahams, T.O., Farayola, O.A., Amoo, O.O., Ayinla, B.S., Osasona, F. and Atadoga, A., 2024. Continuous improvement in information security: A review of lessons from superannuation cybersecurity uplift programs. International Journal of Science and Research Archive, 11(1), pp.1327-1337.
3. Adewusi, A.O., Okoli, U.I., Olorunsogo, T., Adaga, E., Daraojimba, D.O. and Obi, O.C., 2024. Artificial intelligence in cybersecurity: Protecting national infrastructure: A USA.
4. Allioui, H., & Mourdi, Y. (2023). Exploring the full potentials of IoT for better financial growth and stability: A comprehensive survey. *Sensors*, *23*(19), 8015.
5. An, A. (2022). The Evolution of Cyber security Threats in the Digital Age. *International Journal of Business Management and Visuals, ISSN: 3006-2705*, *5*(2), 22-29.
6. Andrea, C. (2017). Hybrid ports: the role of IoT and Cyber Security in the next decade. *Journal of Sustainable Development of Transport and Logistics*, *2*(2 (3)), 47-56.
7. Atadoga, A., Osasona, F., Amoo, O.O., Farayola, O.A., Ayinla, B.S. and Abrahams, T.O., 2024. THE ROLE OF IT IN ENHANCING SUPPLY CHAIN RESILIENCE: A GLOBAL REVIEW. International Journal of Management & Entrepreneurship Research, 6(2), pp.336-351.
8. Azapagic, A. (2003). Systems approach to corporate sustainability: a general management framework. *Process Safety and Environmental Protection*, *81*(5), 303-316.
9. Blom, T., & Niemann, W. (2022). Managing reputational risk during supply chain disruption recovery: A triadic logistics outsourcing perspective.
10. Bozkus Kahyaoglu, S., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial auditing journal*, *33*(4), 360-376.
11. Brewer, R. (2016). Ransomware attacks: detection, prevention and cure. *Network security*, *2016*(9), 5-9.
12. Campbell, C. C. (2019). Solutions for counteracting human deception in social engineering attacks. *Information Technology & People*, *32*(5), 1130-1152.
13. Cihat, A. Ş. A. N. (2023). THE ROLE OF CYBER SITUATIONAL AWARENESS OF HUMANS IN SOCIAL ENGINEERING CYBER ATTACKS ON THE MARITIME DOMAIN. *Mersin University Journal of Maritime Faculty*, *5*(2), 22-36.
14. Das, S., & Mukherjee, S. (2024). Navigating Cloud Security Risks, Threats, and Solutions for Seamless Business Logistics. In *Emerging Technologies and Security in Cloud Computing* (pp. 252-275). IGI Global.
15. Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences*, *11*(10), 4580.
16. Goodall, J. R., Ragan, E. D., Steed, C. A., Reed, J. W., Richardson, G. D., Huffer, K. M., ... & Laska, J. A. (2018). Situ: Identifying and explaining suspicious behavior in networks. *IEEE transactions on visualization and computer graphics*, *25*(1), 204-214.
17. Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications*, *28*, 3629-3654.
18. Heikkilä, J. (2002). From supply to demand chain management: efficiency and customer satisfaction. *Journal of operations management*, *20*(6), 747-767.
19. Kaiser, T., Siddiqua, R., & Hasan, M. M. U. (2022). *A multi-layer security system for data access control, authentication, and authorization* (Doctoral dissertation, Brac University).
20. Keskin, O. F., Caramancion, K. M., Tatar, I., Raza, O., & Tatar, U. (2021). Cyber third-party risk management: A comparison of non-intrusive risk scoring reports. *Electronics*, *10*(10), 1168.
21. Lekota, F., & Coetzee, M. (2019). Cybersecurity incident response for the sub-saharan African aviation industry. In *International Conference on Cyber Warfare and Security* (pp. 536-XII). Academic Conferences International Limited.
22. Leo, P., Isik, Ö., & Muhly, F. (2022). The ransomware dilemma. *MIT Sloan Management Review*, *63*(4), 13-15.
23. Li, Y., Chen, K., Collignon, S., & Ivanov, D. (2021). Ripple effect in the supply chain network: Forward and backward disruption propagation, network health and firm vulnerability. *European Journal of Operational Research*, *291*(3), 1117-1131.

24. Luo, Y. (2022). A general framework of digitization risks in international business. *Journal of international business studies*, *53*(2), 344-361.
25. Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P., & Ni, W. (2018). Anatomy of threats to the internet of things. *IEEE communications surveys & tutorials*, *21*(2), 1636-1675.
26. Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P., & Ni, W. (2018). Anatomy of threats to the internet of things. *IEEE communications surveys & tutorials*, *21*(2), 1636-1675.
27. Mughal, A. A. (2018). The Art of Cybersecurity: Defense in Depth Strategy for Robust Protection. *International Journal of Intelligent Automation and Computing*, *1*(1), 1-20.
28. Okoli, U.I., Obi, O.C., Adewusi, A.O. and Abrahams, T.O., 2024. Machine learning in cybersecurity: A review of threat detection and defense mechanisms.
29. Pandey, S., Singh, R. K., Gunasekaran, A., & Kaushik, A. (2020). Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing*, *13*(1), 103-128.
30. Patel, K. R. (2023). Enhancing Global Supply Chain Resilience: Effective Strategies for Mitigating Disruptions in an Interconnected World. *BULLET: Jurnal Multidisiplin Ilmu*, *2*(1), 257-264.
31. Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*. CRC press.
32. Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the cyber security. *International Journal of scientific research and management*, *9*(12), 669-710.
33. Plachkinova, M., & Knapp, K. (2023). Least Privilege across People, Process, and Technology: Endpoint Security Framework. *Journal of Computer Information Systems*, *63*(5), 1153-1165
34. Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability*, *15*(18), 13369.
35. Saini, H., & Saini, D. (2007). Proactive cyber defense and reconfigurable framework for cyber security. *strategies*, *2*, 3.
36. Serôdio, C., Cunha, J., Candela, G., Rodriguez, S., Sousa, X. R., & Branco, F. (2023). The 6G Ecosystem as Support for IoE and Private Networks: Vision, Requirements, and Challenges. *Future Internet*, *15*(11), 348.
37. Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, *60*, 154-176.
38. Snyder, D. L. (2022). *A Qualitative Meta-synthesis on the Benefits of Planning for Ransomware Attacks at a Strategic Organizational Level* (Doctoral dissertation, Colorado Technical University).
39. Sobb, T., Turnbull, B., & Moustafa, N. (2020). Supply chain 4.0: A survey of cyber security challenges, solutions and future directions. *Electronics*, *9*(11), 1864.
40. Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., & Lopez, J. (2018). A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Communications Surveys & Tutorials*, *20*(4), 3453-3495.
41. Sullivan, D. (2005). *The definitive guide to controlling malware, spyware, phishing, and spam*. Realtimepublishers. com.
42. Tien, N. H., Anh, D. B. H., & Thuc, T. D. (2019). Global supply chain and logistics management.
43. Tseng, Y. Y., Yue, W. L., & Taylor, M. A. (2005). The role of transportation in logistics chain. Eastern Asia Society for Transportation Studies.
44. Yathiraju, N. (2022). Investigating the use of an artificial intelligence model in an ERP cloud-based system. *International Journal of Electrical, Electronics and Computers*, *7*(2), 1-26.
45. Yeboah-Ofori, A., Islam, S., Lee, S. W., Shamszaman, Z. U., Muhammad, K., Altaf, M., & Al-Rakhami, M. S. (2021). Cyber threat predictive analytics for improving cyber supply chain security. *IEEE Access*, *9*, 94318-94337.