World Journal of
Advanced Science and Tehnology

Journal homepage: https://zealjournals.com/wjast/

(REVIEW ARTICLE)

Check for updates

Securing the digital supply chain: Cybersecurity best practices for logistics and shipping companies

Agnes Clare Odimarha [1,*], Sodrudeen Abolore Ayodeji [2] and Emmanuel Adeyemi Abaku [3]

[1] *Shell Nigeria.*
[2] *Matrix Limited Energy, Lagos, Nigeria.*
[3] *Gerald and Gerald Exchanges, Lagos, Nigeria.*

World Journal of Advanced Science and Technology, 2024, 05(01), 026–033

Publication history: Received on 10 February 2024; revised on 21 March 2024; accepted on 23 March 2024

Article DOI: https://doi.org/10.53346/wjast.2024.5.1.0030

Abstract

The review investigates the pressing need for robust cybersecurity measures within the logistics and shipping sector, where the digital supply chain is vulnerable to a myriad of cyber threats. The paper delves into the specific challenges faced by logistics companies, including the interconnectedness of global supply chains, reliance on digital technologies for operations, and the high value of goods in transit. It explores the multifaceted nature of cyber risks, encompassing threats such as ransomware, phishing attacks, data breaches, and supply chain disruptions, which can have far-reaching consequences for business continuity and reputation. Through a detailed analysis, the study elucidates cybersecurity best practices tailored to the logistics and shipping industry, encompassing both technical solutions and organizational policies. These include implementing robust authentication and access controls, encrypting sensitive data in transit and at rest, establishing secure communication channels, and conducting regular vulnerability assessments and penetration testing. Furthermore, the paper emphasizes the importance of fostering a culture of cybersecurity awareness among employees through comprehensive training programs and incident response drills. It also discusses the role of regulatory compliance frameworks such as GDPR, CCPA, and industry-specific standards like ISO 27001 in guiding cybersecurity efforts and ensuring adherence to best practices. By providing actionable recommendations and insights garnered from real-world case studies, the study equips logistics and shipping companies with the knowledge and tools needed to bolster their cybersecurity defenses, safeguard critical assets, and maintain trust in the digital supply chain ecosystem.

Keywords: Secure; Digital; Supply Chain; Cybersecurity; Logistics; Shipping Companies.

1. Introduction

The term "digital supply chain" refers to the integration of digital technologies and information systems across the entire supply chain process, encompassing the planning, sourcing, manufacturing, logistics, and distribution stages (MacCarthy and Ivanov, 2022). Unlike traditional supply chains, which often rely on manual processes and paper-based documentation, the digital supply chain leverages technologies such as IoT (Internet of Things), cloud computing, big data analytics, and interconnected systems to enhance efficiency, visibility, and collaboration. In the context of logistics and shipping, the digital supply chain involves the seamless exchange of data and information between various stakeholders, including manufacturers, suppliers, carriers, distributors, and retailers. This interconnected approach enables real-time tracking, data-driven decision-making, and optimized resource utilization throughout the supply chain, ultimately improving the overall operational performance (Ejairu et al., 2024).

* Corresponding author: Agnes Clare Odimarha

As businesses increasingly rely on digital technologies to streamline their supply chain operations, the importance of securing the digital supply chain becomes paramount (Atadoga et al., 2024). The interconnected nature of the digital supply chain introduces a multitude of vulnerabilities that can be exploited by cyber threats. The potential consequences of a cybersecurity breach in the supply chain include disruptions to operations, loss of sensitive data, financial losses, reputational damage, and even compromise of customer trust (Pandey et al., 2020). Securing the digital supply chain is crucial for maintaining the integrity and confidentiality of sensitive information, ensuring the continuity of operations, and safeguarding the overall resilience of the supply chain ecosystem. With the increasing frequency and sophistication of cyber attacks, organizations in the logistics and shipping industry must proactively implement robust cybersecurity measures to protect their digital assets and maintain a competitive edge in the modern business landscape (Ahmad et al., 2024).

The logistics and shipping industry faces unique cybersecurity challenges due to the complex and dynamic nature of its operations (Ahmad et al., 2024). With a diverse range of stakeholders involved in the supply chain, phishing attacks targeting employees, suppliers, and partners can compromise sensitive information and provide unauthorized access to critical systems (Ogedengbe et al., 2024). The prevalence of ransomware poses a significant threat to logistics companies, as it can lead to the encryption of essential data, disrupting operations and demanding financial payments for decryption keys. Malicious or unintentional actions by employees within logistics companies can pose a substantial risk, emphasizing the need for robust access controls and employee awareness programs. Cybercriminals often target vulnerabilities in the supply chain to compromise the integrity of products or services, leading to potential financial losses and damage to the organization's reputation (Pandey et al., 2020). Understanding and addressing these challenges is crucial for developing effective cybersecurity strategies tailored to the unique needs of logistics and shipping companies.

1.1. Threat landscape

The logistics industry, operating within the expansive and interconnected digital supply chain, is susceptible to a range of cybersecurity threats that can have far-reaching consequences (Okoli et al., 2024). Understanding these threats is essential for developing effective security measures. Here are some common threats faced by logistics companies:

1.1.1. Phishing Attacks

Phishing attacks involve the use of deceptive emails, messages, or websites to trick individuals into revealing sensitive information such as login credentials or financial data (Alkhalil et al., 2021). Given the diverse range of stakeholders involved in logistics, including employees, suppliers, and partners, phishing attacks pose a significant risk. Successful phishing attacks can lead to unauthorized access to critical systems, compromise of sensitive information, and potential disruptions to supply chain operations (Okoye et al., 2024).

Ransomware is a type of malware that encrypts files or entire systems, demanding a ransom payment for the decryption key. The critical nature of logistics operations makes ransomware a potent threat, as an attack can disrupt the movement of goods, compromise tracking systems, and halt essential services. Ransomware attacks can result in downtime, financial losses, reputational damage, and the potential leakage of sensitive data, affecting both internal operations and relationships with customers and partners.

Insider threats involve individuals within an organization who, intentionally or unintentionally, pose a risk to the security of systems and data. Insider threats may come from employees with access to sensitive logistics information, either through malicious actions or unintentional mistakes. Insider threats can lead to data breaches, unauthorized access, and disruptions in logistics operations. Malicious insiders may intentionally compromise systems, while unintentional mistakes can result in accidental data leaks.

Supply chain attacks target vulnerabilities within the supply chain, aiming to compromise the integrity of products or services. Logistics companies are integral parts of the supply chain, making them potential targets for cybercriminals seeking to exploit weaknesses in transportation, warehousing, and distribution. Supply chain attacks can lead to the distribution of compromised products, disruptions in the delivery process, and damage to the reputation of logistics companies (Okoye et al., 2024). The interconnected nature of the supply chain amplifies the ripple effects of such attacks.

1.1.2. Case Studies Highlighting Cybersecurity Incidents in Logistics

Maersk, one of the world's largest shipping companies, fell victim to the NotPetya ransomware attack in 2017. The malware spread through the company's network, leading to widespread system outages and disrupting global shipping

operations. Maersk reported losses of hundreds of millions of dollars due to the incident, highlighting the severe financial consequences of a cybersecurity breach in the logistics sector (Barthwal and Agarwala, 2017).

Numerous logistics companies have faced targeted phishing attacks, with cybercriminals impersonating employees, suppliers, or partners to gain unauthorized access or extract sensitive information. These attacks often result in compromised login credentials, unauthorized access to logistics systems, and potential data breaches, emphasizing the ongoing threat posed by phishing in the industry (Maurushat et al., 2019).

1.2. Cybersecurity best practices

1.2.1. Employee Training and Awareness

Conduct regular phishing awareness programs to educate employees about the tactics used by cybercriminals (Adewusi et al., 2024). Simulated phishing exercises can help employees recognize and avoid phishing attempts. By enhancing employees' ability to identify phishing attacks, organizations can reduce the risk of unauthorized access and data breaches. Provide comprehensive cybersecurity training sessions for employees, covering topics such as password hygiene, secure browsing practices, and the importance of reporting suspicious activities (Abrahams et al., 2024). Ongoing training ensures that employees stay informed about the latest cybersecurity threats and best practices, fostering a proactive security mindset. Foster a security-conscious culture within the organization by promoting cybersecurity as a shared responsibility. Encourage employees to report security incidents promptly and create a non-punitive environment for reporting. A culture of cybersecurity awareness helps create a collective defense mechanism, making employees an integral part of the organization's overall security posture (Fisher et al., 2021).

1.2.2. Network Security

Implement a secure network architecture with proper segmentation to limit lateral movement in case of a breach. Utilize firewalls and routers to control traffic and deploy virtual private networks (VPNs) for secure remote access (Nyakomitta and Abeka, 2020). A robust network architecture ensures that unauthorized access is restricted, reducing the potential impact of cyber attacks on critical systems. Deploy firewalls and intrusion detection/prevention systems to monitor network traffic for malicious activities. Configure these systems to block or alert on suspicious behavior. Firewalls and intrusion prevention systems act as the first line of defense, preventing unauthorized access and detecting and mitigating potential threats in real time (Thapa and Mailewa, 2020). Conduct regular network assessments and audits to identify vulnerabilities and ensure compliance with security policies. Penetration testing can simulate real-world attacks to evaluate the effectiveness of security measures. Continuous assessments help organizations proactively address network weaknesses, reducing the likelihood of successful cyber attacks (Okoli et al., 2024).

1.2.3. Endpoint Security

Install and regularly update endpoint protection software to detect and prevent malware, ransomware, and other malicious activities on devices (Ren et al., 2020). Endpoint protection safeguards individual devices, including computers and laptops, preventing the spread of malware and enhancing the overall security posture. Implement device encryption to protect sensitive data stored on endpoints. Full disk encryption ensures that even if a device is lost or stolen, the data remains inaccessible to unauthorized individuals (Scarfone et al., 2007). Encryption adds an additional layer of security, safeguarding data from potential breaches and complying with data protection regulations. Mobile Device Management (MDM) Solutions to manage and secure mobile devices accessing corporate networks. Implement policies for device configuration, application management, and remote wiping in case of loss or theft. With the increasing use of mobile devices, MDM solutions help enforce security policies, protect sensitive information, and maintain control over corporate data (Doghudje and Akande, 2023).

1.2.4. Data Protection

Encrypt data both in transit and at rest to prevent unauthorized access. Use secure protocols for data transmission and implement encryption algorithms for stored data (Sharma and Kakkar, 2012). Encryption safeguards sensitive information, mitigating the risk of data interception during transmission and protecting data stored on servers or devices. Establish a routine backup schedule for critical data. Regularly test and verify the integrity of backups to ensure quick data recovery in the event of a cyber attack or system failure. Data backups serve as a crucial recovery mechanism, enabling organizations to restore operations and minimize the impact of data loss caused by cyber incidents. Implement robust access controls, granting employees the minimum level of access required to perform their job functions. Enforce the principle of least privilege to limit potential damage from insider threats. Strict access controls reduce the attack surface and mitigate the risk of unauthorized access, minimizing the potential impact of security incidents (Veshne, 2023).

1.2.5. Supply Chain Security

Vendor Risk Assessments, conduct thorough risk assessments of vendors and suppliers before entering into partnerships. Evaluate their cybersecurity practices, including data protection measures and adherence to security standards (Ookye et al., 2024). Assessing vendor risks helps ensure that third-party relationships do not introduce vulnerabilities into the supply chain, enhancing overall cybersecurity resilience. Third-Party Security Audits, perform regular security audits on third-party vendors to validate their adherence to agreed-upon security standards. Address any identified vulnerabilities or weaknesses promptly. Continuous monitoring and auditing of third-party security practices help maintain a secure supply chain ecosystem and protect against potential security breaches (Hassija et al., 2020). Establishing Secure Communication Channels with Suppliers, implement secure communication channels, such as encrypted emails and file transfers, when exchanging sensitive information with suppliers (Atadoga et al., 2024). Clearly communicate security expectations to suppliers. Secure communication channels safeguard the confidentiality of information exchanged with suppliers, preventing unauthorized access and potential data breaches.

1.2.6. Incident Response Plan

Form an incident response team consisting of individuals with expertise in cybersecurity, IT, legal, and communication. Clearly define roles and responsibilities within the team. A dedicated incident response team ensures a coordinated and efficient response to cybersecurity incidents, minimizing downtime and potential damages. Develop a comprehensive incident response plan outlining the step-by-step procedures to follow in the event of a cybersecurity incident (van der Kleij et al., 2022). Define communication protocols, escalation procedures, and recovery processes. Having a well-documented incident response plan ensures a swift and organized response to cyber threats, reducing the impact of incidents on the organization. Conduct regular drills and simulations to test the effectiveness of the incident response plan. Evaluate the team's readiness to handle various cybersecurity scenarios and identify areas for improvement (Amoo et al., 2024). Regular exercises help refine incident response procedures, familiarize team members with their roles, and improve overall incident response capabilities.

1.2.7. Compliance and Regulations

Stay informed about industry-specific regulations and standards related to cybersecurity in logistics and shipping. Develop processes to ensure compliance with relevant regulatory requirements. Compliance with industry regulations not only helps avoid legal repercussions but also ensures that cybersecurity measures align with industry best practices (Amoo et al., 2024). Adhere to specific compliance standards such as GDPR (General Data Protection Regulation) or HIPAA (Health Insurance Portability and Accountability Act), depending on the nature of the data being handled (Determann, 2019). Compliance with data protection regulations is essential for protecting customer information, avoiding fines, and maintaining trust in the logistics and shipping industry. Conduct regular assessments to ensure ongoing compliance with industry regulations and standards. Identify and address any gaps or areas of non-compliance promptly. Regular assessments help organizations stay proactive in meeting regulatory requirements, reducing the risk of legal consequences and reputational damage (Rayner, 2004).

1.2.8. Continuous Monitoring and Threat Intelligence

Deploy continuous monitoring tools that provide real-time visibility into network activities, system logs, and user behavior. Utilize intrusion detection systems and security information and event management (SIEM) solutions (Muhammad et al., 2023). Continuous monitoring allows organizations to detect and respond to cybersecurity threats promptly, minimizing the potential impact of security incidents. Subscribe to threat intelligence feeds to stay informed about the latest cybersecurity threats and attack trends. Integrate threat intelligence into security operations for proactive defense. Threat intelligence enhances the organization's ability to anticipate and respond to emerging cyber threats, allowing for a more proactive cybersecurity posture (Sun et al., 2023). Regularly participate in industry forums, conferences, and cybersecurity communities to stay informed about emerging threats and vulnerabilities relevant to the logistics and shipping sector. Staying informed about the evolving threat landscape helps organizations adapt their cybersecurity strategies to address new and emerging challenges effectively.

1.2.9. Technology Updates and Patch Management

Implement a robust patch management process to ensure that software, operating systems, and applications are regularly updated with the latest security patches (Li and Paxson, 2017). Timely software updates and patching mitigate the risk of exploiting known vulnerabilities, reducing the likelihood of successful cyber attacks. Conduct regular vulnerability assessments to identify and prioritize potential weaknesses in systems and applications. Develop and implement a plan to address and remediate identified vulnerabilities. Proactive vulnerability management helps organizations address potential security risks before they can be exploited by cybercriminals, enhancing overall

cybersecurity resilience (Green et al., 2020). Identify and phase out outdated or unsupported technology within the organization. Replace legacy systems with modern, secure alternatives to reduce the risk of vulnerabilities. Outdated technology poses a higher risk of security vulnerabilities. Timely retirement ensures that the organization maintains a secure and up-to-date technology infrastructure. Implementing these cybersecurity best practices provides logistics and shipping companies with a comprehensive framework for enhancing their security posture in the digital supply chain. A holistic approach that combines employee awareness, robust technical measures, supply chain resilience, and compliance adherence is essential for mitigating cybersecurity risks and maintaining the integrity of operations (Colicchia et al., 2019). By continuously evolving and adapting to the dynamic threat landscape, organizations can foster a secure and resilient digital supply chain ecosystem.

1.3. Case studies

1.3.1. Successful Cybersecurity Implementations in Logistics

FedEx, a global courier delivery services company, has implemented robust cybersecurity measures to protect its extensive logistics network. The company utilizes advanced encryption technologies to secure data in transit and at rest. Additionally, FedEx employs comprehensive network monitoring and intrusion detection systems to detect and mitigate potential threats in real-time. FedEx's success in cybersecurity is attributed to a combination of cutting-edge technologies, regular security audits, and a proactive approach to threat intelligence. The company prioritizes employee training on cybersecurity best practices and maintains a strong culture of security awareness (Kern, 2021).

DHL Supply Chain, a division of the global logistics company DHL, has invested in state-of-the-art cybersecurity solutions to protect its supply chain operations. The company emphasizes secure communication channels with suppliers, conducting thorough vendor risk assessments. DHL Supply Chain also utilizes advanced endpoint protection software to secure devices across its network. DHL Supply Chain's success lies in its holistic approach to cybersecurity, integrating technology, employee training, and robust vendor management practices. The company continuously evaluates and updates its cybersecurity measures to adapt to the evolving threat landscape (Lehmacher, 2017).

1.3.2. Lessons Learned from Cybersecurity Incidents

Maersk Cyber Attack (2017), Maersk, a leading shipping company, experienced a significant cybersecurity incident when it fell victim to the NotPetya ransomware attack in 2017. The malware spread rapidly, impacting operations globally and causing extensive disruptions. The incident highlighted the critical importance of maintaining regular and reliable data backups. Organizations should ensure the integrity and accessibility of backup systems to facilitate quick recovery in the event of a cyber attack. The incident underscored the necessity of having a well-defined and tested incident response plan. Maersk's response was hindered by the lack of a comprehensive plan, emphasizing the importance of proactive incident response preparedness (Schwarz et al., 2021).

Targeted Phishing in Logistics Companies (Ongoing), Numerous logistics companies have faced targeted phishing attacks, with cybercriminals impersonating employees, suppliers, or partners to gain unauthorized access or extract sensitive information. The incidents emphasize the ongoing need for phishing awareness programs and regular cybersecurity training for employees. Enhancing the ability of staff to recognize and report phishing attempts is crucial in preventing unauthorized access. Ensuring secure communication channels, especially in interactions with external parties, is vital. Companies need to establish and enforce secure communication protocols to protect sensitive information from compromise (Maurushat et al., 2019).

1.3.3. Continuous Improvement Strategies

Integrate threat intelligence feeds into cybersecurity operations to stay informed about emerging threats and vulnerabilities (Sun et al., 2023). Implementing a threat intelligence-driven approach allows organizations to proactively adjust their security measures based on real-time insights. Enhances the organization's ability to anticipate and respond to evolving cyber threats, reducing the likelihood of successful attacks and improving overall cybersecurity resilience. Conduct regular security audits and vulnerability assessments to identify weaknesses in the cybersecurity posture (Al-Karaki et al., 2022). This continuous evaluation allows organizations to address emerging risks promptly and implement necessary improvements. Provides a proactive mechanism for identifying and mitigating potential vulnerabilities, reducing the likelihood of successful cyber attacks and ensuring the organization's security measures remain robust. Foster a culture of continuous learning and adaptability within the organization. Encourage employees to stay informed about the latest cybersecurity trends, threats, and best practices through training, workshops, and industry engagement. Employees who are well-informed about cybersecurity contribute actively to the organization's security posture (Nikel and Amaechi, 2022). A culture of continuous learning ensures that the workforce remains vigilant and responsive to evolving cyber threats. Regularly review and refine the incident response plan based on

lessons learned from simulations, drills, and actual incidents. Ensure that the plan remains up-to-date, aligns with the current threat landscape, and incorporates feedback from incident response exercises. A well-maintained incident response plan enhances the organization's ability to handle cybersecurity incidents effectively. Continuous refinement ensures that the plan remains relevant and responsive to emerging threats. Collaborate with industry peers, cybersecurity experts, and information-sharing platforms to stay informed about industry-specific threats and mitigation strategies (Rodin, 2015). Participate in forums, conferences, and collaborative initiatives to share insights and best practices. Industry collaboration provides access to valuable threat intelligence, fosters shared learning, and strengthens the collective cybersecurity defense of the logistics and shipping sector. Continuous improvement in cybersecurity is an ongoing necessity for logistics and shipping companies. Learning from successful implementations, understanding lessons from incidents, and implementing strategies for continuous enhancement ensures a resilient and adaptive cybersecurity posture. By combining technological innovation, employee empowerment, and industry collaboration, organizations can navigate the dynamic cybersecurity landscape and safeguard the integrity of their digital supply chain operations (Chisty et al., 2022).

2. Conclusion

In navigating the complex and interconnected landscape of the digital supply chain, logistics and shipping companies must adhere to key cybersecurity best practices to protect their operations, data, and reputation. It is crucial to emphasize that cybersecurity is not a one-time effort but an ongoing and dynamic process. The digital supply chain is continuously evolving, and so too must the cybersecurity measures put in place. Threat landscapes change, new vulnerabilities emerge, and cybercriminal tactics evolve. Therefore, organizations must remain vigilant, adapt to emerging challenges, and continuously enhance their cybersecurity posture. Regular training sessions, updates to policies and procedures, and periodic assessments are essential components of maintaining a strong cybersecurity stance. The development and refinement of incident response plans should be ongoing, with lessons learned from each incident feeding into continuous improvement efforts. Additionally, staying informed about emerging technologies, threats, and best practices are key elements of a proactive and adaptive cybersecurity strategy. Collaboration within the logistics and shipping industry is paramount to building a collective defense against cyber threats. Cybersecurity is a shared responsibility, and the interconnected nature of the digital supply chain necessitates a united front against potential adversaries. Key points for fostering collaboration include:

Encourage the sharing of threat intelligence and best practices among industry peers. This collaboration can help organizations stay ahead of emerging threats and vulnerabilities. Collaborate on training initiatives and awareness programs. Shared resources and knowledge can enhance the cybersecurity skills of the industry workforce, creating a more resilient collective defense. Establish frameworks for coordinated responses to cyber incidents. In the event of a widespread attack targeting the industry, a unified response can mitigate the impact and speed up recovery efforts. Work together to establish and adhere to industry-wide cybersecurity standards and guidelines. A common framework can elevate the overall security posture of the entire logistics and shipping ecosystem. Collaborate in advocating for regulatory measures that promote cybersecurity in the industry. This could include industry-specific regulations that set a baseline for cybersecurity practices and standards.

By fostering a collaborative environment, logistics and shipping companies can create a collective defense that is more resilient, adaptive, and capable of addressing the evolving challenges posed by cyber threats. Together, organizations can strengthen the overall cybersecurity posture of the industry and ensure the continued integrity and security of the digital supply chain.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] 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.

[2] Abrahams, T.O., Farayola, O.A., Kaggwa, S., Uwaoma, P.U., Hassan, A.O. and Dawodu, S.O., 2024. CYBERSECURITY AWARENESS AND EDUCATION PROGRAMS: A REVIEW OF EMPLOYEE ENGAGEMENT AND ACCOUNTABILITY. Computer Science & IT Research Journal, 5(1), pp.100-119.

[3] Abrahams, T.O., Farayola, O.A., Kaggwa, S., Uwaoma, P.U., Hassan, A.O. and Dawodu, S.O., 2024. REVIEWING THIRD-PARTY RISK MANAGEMENT: BEST PRACTICES IN ACCOUNTING AND CYBERSECURITY FOR SUPERANNUATION ORGANIZATIONS. Finance & Accounting Research Journal, 6(1), pp.21-39.

[4] 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.

[5] Ahmad, I.A.I., Anyanwu, A.C., Onwusinkwue, S., Dawodu, S.O., Akagha, O.V. and Ejairu, E., 2024. CYBERSECURITY CHALLENGES IN SMART CITIES: A CASE REVIEW OF AFRICAN METROPOLISES. Computer Science & IT Research Journal, 5(2), pp.254-269.

[6] Al-Karaki, J. N., Gawanmeh, A., & El-Yassami, S. (2022). GoSafe: On the practical characterization of the overall security posture of an organization information system using smart auditing and ranking. *Journal of King Saud University-Computer and Information Sciences*, *34*(6), 3079-3095.

[7] Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*, 563060

[8] Amoo, O.O., Atadoga, A., Osasona, F., Abrahams, T.O., Ayinla, B.S. and Farayola, O.A., 2024. GDPR's impact on cybersecurity: A review focusing on USA and European practices. International Journal of Science and Research Archive, 11(1), pp.1338-1347.

[9] Amoo, O.O., Osasona, F., Atadoga, A., Ayinla, B.S., Farayola, O.A. and Abrahams, T.O., 2024. Cybersecurity threats in the age of IoT: A review of protective measures. International Journal of Science and Research Archive, 11(1), pp.1304-1310.

[10] 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.

[11] Barthwal, N., & Agarwala, C. D. N. (2017). Industry 4.0 in the Shipping Industry: Challenges and Preparedness—The Prevailing Scenario. *maritime*, 265.

[12] Chisty, N. M. A., Baddam, P. R., & Amin, R. (2022). Strategic Approaches to Safeguarding the Digital Future: Insights into Next-Generation Cybersecurity. *Engineering International*, *10*(2), 69-84

[13] Colicchia, C., Creazza, A., & Menachof, D. A. (2019). Managing cyber and information risks in supply chains: insights from an exploratory analysis. *Supply Chain Management: An International Journal*, *24*(2), 215-240.

[14] Determann, L. (2019). Healthy data protection. *Mich. Tech. L. Rev.*, *26*, 229.

[15] Doghudje, I., & Akande, O. (2023). Dual User Profiles: A Secure and Streamlined MDM Solution for the Modern Corporate Workforce. *Journal of Intelligent Connectivity and Emerging Technologies*, *8*(4), 15-26.

[16] Ejairu, E., Mhlongo, N.Z., Odeyemi, O., Nwankwo, E.E. and Odunaiya, O.G., 2024. Blockchain in global supply chains: A comparative review of USA and African practices. International Journal of Science and Research Archive, 11(1), pp.2093-2100.

[17] Ejairu, E., Mhlongo, N.Z., Odeyemi, O., Nwankwo, E.E. and Odunaiya, O.G., 2024. Blockchain in global supply chains: A comparative review of USA and African practices. International Journal of Science and Research Archive, 11(1), pp.2093-2100.

[18] Fisher, R., Porod, C., & Peterson, S. (2021). Motivating employees and organizations to adopt a cybersecurity-focused culture. *Journal of Organizational Psychology*, *21*(1), 114-131.

[19] Green, A. W., Woszczynski, A. B., Dodson, K., & Easton, P. (2020). Responding to cybersecurity challenges: Securing vulnerable US emergency alert systems. *Communications of the Association for Information Systems*, *46*(1), 8.

[20] Hassija, V., Chamola, V., Gupta, V., Jain, S., & Guizani, N. (2020). A survey on supply chain security: Application areas, security threats, and solution architectures. *IEEE Internet of Things Journal*, *8*(8), 6222-6246.

[21] Kern, J. (2021). The digital transformation of logistics: A review about technologies and their implementation status. *The digital transformation of logistics: Demystifying impacts of the fourth industrial revolution*, 361-403.

[22] Lehmacher, W. (2017). *The global supply chain*. Springer.

[23] Li, F., & Paxson, V. (2017). A large-scale empirical study of security patches. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (pp. 2201-2215).

[24] MacCarthy, B. L., & Ivanov, D. (2022). The Digital Supply Chain—emergence, concepts, definitions, and technologies. In *The digital supply chain* (pp. 3-24). Elsevier.

[25] Maurushat, A., Bello, A., & Bragg, B. (2019). Artificial intelligence enabled cyber fraud: a detailed look into payment diversion fraud and ransomware. *Indian JL & Tech.*, *15*, 261.

[26] Maurushat, A., Bello, A., & Bragg, B. (2019). Artificial intelligence enabled cyber fraud: a detailed look into payment diversion fraud and ransomware. *Indian JL & Tech.*, *15*, 261.

[27] Muhammad, A. R., Sukarno, P., & Wardana, A. A. (2023). Integrated security information and event management (siem) with intrusion detection system (ids) for live analysis based on machine learning. *Procedia Computer Science*, *217*, 1406-1415.

[28] Nikel, F. H., & Amaechi, A. O. (2022). An Assessment of Employee Knowledge, Awareness, Attitude towards Organizational Cybersecurity in Cameroon. *Netw. Commun. Technol.*, *7*(1), 1-11.

[29] Nwankwo, T.C., Ejairu, E., Awonuga, K.F. and Oluwadamilare, F., 2024. Conceptualizing sustainable supply chain resilience: Critical materials manufacturing in Africa as a catalyst for change.

[30] Nyakomitta, P. S., & Abeka, S. O. (2020). Security investigation on remote access methods of virtual private network. *Global journal of computer science and technology*, *20*.

[31] Ogedengbe, D.E., Oladapo, J.O., Elufioye, O.A., Ejairu, E. and Ezeafulukwe, C., 2024. Strategic HRM in the logistics and shipping sector: Challenges and opportunities.

[32] 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.

[33] 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.

[34] Okoye, C.C., Ofodile, O.C., Tula, S.T., Nifise, A.O.A., Falaiye, T., Ejairu, E. and Addy, W.A., 2024. Risk management in international supply chains: A review with USA and African Cases. Magna Scientia Advanced Research and Reviews, 10(1), pp.256-264.

[35] 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.

[36] 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.

[37] Rayner, J. (2004). *Managing reputational risk: Curbing threats, leveraging opportunities*. John Wiley & Sons.

[38] Ren, A., Liang, C., Hyug, I., Broh, S., & Jhanjhi, N. Z. (2020). A three-level ransomware detection and prevention mechanism. *EAI Endorsed Transactions on Energy Web*, *7*(26).

[39] Rodin, D. N. (2015). The cybersecurity partnership: A proposal for cyberthreat information sharing between contractors and the federal government. *Public Contract Law Journal*, *44*(3), 505-528.

[40] Scarfone, K., Souppaya, M., & Sexton, M. (2007). Guide to storage encryption technologies for end user devices. *NIST Special Publication*, *800*(S 111).

[41] Schwarz, M., Marx, M., & Federrath, H. (2021). A structured analysis of information security incidents in the maritime sector. *arXiv preprint arXiv:2112.06545*

[42] Sharma, G., & Kakkar, A. (2012). Cryptography Algorithms and approaches used for data security. *International Journal of Scientific & Engineering Research*, *3*(6), 1-6.

[43] Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y., & Zhang, J. (2023). Cyber threat intelligence mining for proactive cybersecurity defense: a survey and new perspectives. *IEEE Communications Surveys & Tutorials*.

[44] Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y., & Zhang, J. (2023). Cyber threat intelligence mining for proactive cybersecurity defense: a survey and new perspectives. *IEEE Communications Surveys & Tutorials*.

[45] Thapa, S., & Mailewa, A. (2020). The role of intrusion detection/prevention systems in modern computer networks: A review. In *Conference: Midwest Instruction and Computing Symposium (MICS)* (Vol. 53, pp. 1-14).

[46] van der Kleij, R., Schraagen, J. M., Cadet, B., & Young, H. (2022). Developing decision support for cybersecurity threat and incident managers. *Computers & Security*, *113*, 102535.

[47] Veshne, J. (2023). Attack Surface Management: Principles for simplifying the complexity of OT security.