Supply Chain Digitalization and Vulnerability to Cyber Risks

MUSA Tahir Ibrahim[1],ODEH Godfrey Ofukwu[2]

SEMINAR Phd/M.Phil. Supply Chain Management Institute of Governance and Development Studies Nasarawa State University, Keffi-Nigeria.

DOI: https://doi.org/10.47772/IJRISS.2026.10100301

Received: 20 January 2026; Accepted: 25 January 2026; Published: 04 February 2026

ABSTRACT

The rapidly evolving digitalization of supply chains has transformed traditional procurement processes, thereby enhancing efficiency and collaboration. However, this increased reliance on digital technologies exposes organizations to heightened cyber risks. This conceptual paper qims to explore the double-edged sword of supply chain digitalization (SCD): While SCD, offers significant benefits in efficiency and transparency, it also introduces and increases the vulnerability to cyber risks. Leveraging concepts from Supply Chain Management (SCM), Information Systems (IS), and Cybersecurity, this paper develops a basis to understand how the adoption of key digital technologies—such as the Internet of Things (IoT), Blockchain, Cloud Computing, and Enterprise Resource Planning (ERP) systems—widens the cyber-attack surface. This is particularly critical in a developing country like Nigeria, where challenges like inadequate digital infrastructure, limited cybersecurity skills, and evolving regulatory environment worsen inherent weaknesses. We discuss the potential consequences and suggest a theoretical model for developing cyber-resilient digital supply chains, and providing a groundwork for future empirical research. In addition, we discussed concepts of Technology-Organization-Environment (TOE) framework, combined with elements of organizational Resilience Theory (Sheffi, 2015). The TOE framework suggests that technology adoption is influenced by the technological setting, the organizational readiness, and the environmental pressures. We extend this by arguing that in a high-risk environment (the 'E' factor, which includes the cyber threat environment), the adoption of technology (SCD) must be balanced against the resulting system exposure (Vulnerability to cyber-risks -VCR).

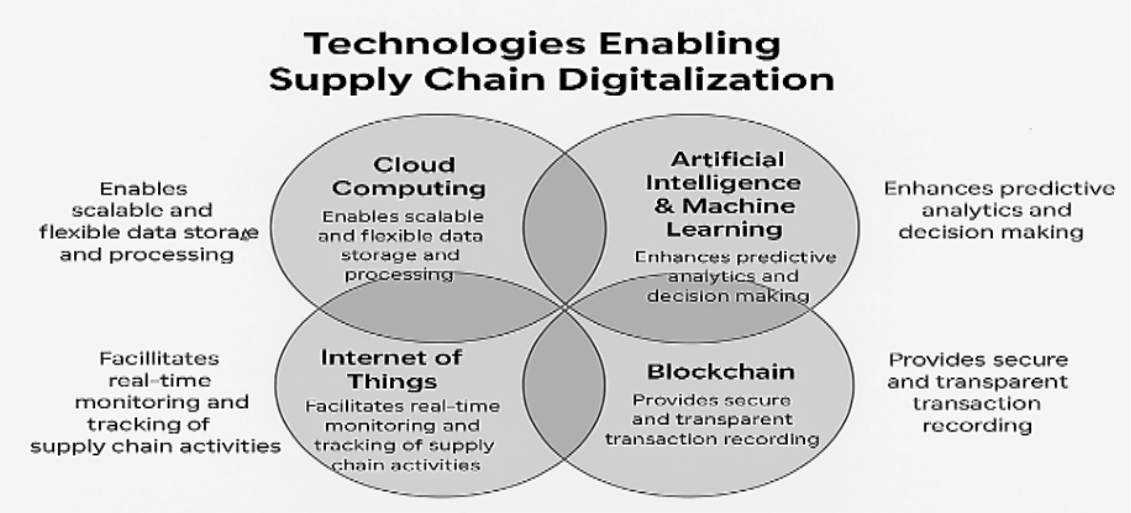
Keywords: Digitalization, Vulnerability, Cyber Risks, Resilience.

INTRODUCTION

The rapid shift to Industry 4.0 demands supply chain digitalization (SCD) for global competitiveness, especially in oil-driven economies like Nigeria with fragmented logistics. Large firms, ports, and logistics players are adopting tools like IoT, AI, blockchain, and cloud computing to replace manual processes with real-time, data driven systems (Akinwumi, 2022; Ivanov et al., 2022; Büyüközkan & Göçer, 2018). While SCD enhances visibility and agility, it heightens vulnerability to cyber risks (VCR) such as breaches, ransomware, and disruptions in Nigeria's high-threat landscape of cyber syndicates and infrastructure gaps (He & Wang, 2021; Uzor & Chinedu, 2023; Adebayo & Ojo, 2020).

This paper reviews literature on SCD's link to VCR in emerging economies, focusing on Nigeria's critical sectors (oil & gas, banking, telecoms), and explores the research question: How does digital technology adoption in supply chains affect cyber risk vulnerability, and what moderates this relationship?

Figure 1



Note: This figure illustrates four key technologies that enable supply chain digitalization

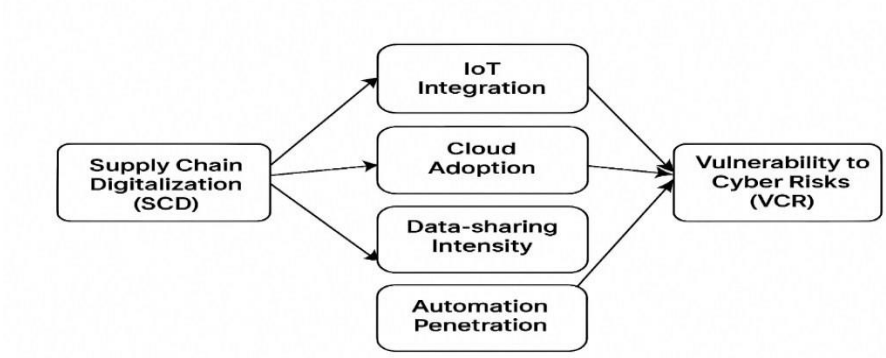
LITERATURE REVIEW

Earlier research modeled cyber risk mainly as an information technology security issue. However, significant works by Bocek et al. (2017) on blockchain and Ivanov et al. (2019) on digital supply chain twins shifted this paradigm, positioning cyber risk as a systemic operational and strategic threat. The Resource-Based View (RBV) explains how digital assets can become sources of vulnerability if not protected, while Network Theory illuminates how interdependencies in digital supply chains facilitate the propagation of cyber incidents from a single weak link (e.g., a small vendor with poor security) to entire networks. More recently, the Dynamic Capabilities lens has been employed to analyze how firms can reconfigure processes for cyber resilience. The Technology-Organization-Environment (TOE) model and the Socio-Technical Systems Theory, highlighted the relationship between technological innovation, organizational readiness, and environmental factors (Tornatzky & Fleischer, 1990; Bostrom & Heinen, 1977). These models suggest that digitalization enhances interconnectivity and data exchange, increasing the attack surface for cyber threats (Ivanov et al., 2022).

In the Nigerian context, exceptional challenges emanate from infrastructural deficits, inadequate cybersecurity awareness, and regulatory gaps (Adebayo & Ojo, 2020). The theoretical literature emphasizes that supply chains in Nigeria are particularly vulnerable to risks due to legacy systems, fragmented digital implementation, and the prevalence of informal networks (Olumide & Adekunle, 2021). As digitalization accelerates, the need for robust risk management frameworks and capacity-building initiatives becomes paramount.

Conceptual Model and Propositions

Figure 2 Conceptual Model Linking Supply Chain Digitalization (SCD) to Vulnerability to Cyber Risks (VCR)



Conceptual Model Overview

This model proposes a positive relationship between supply chain digitalization (SCD) and vulnerability to cyber risks (VCR) in Nigerian firms. SCD elevates VCR through four key proxies: IoT integration, cloud adoption, data-sharing intensity, and automation penetration. These mechanisms arise from increased connectivity and interdependence, creating more entry points for cyber threats.

Key Technology Proxies and Impacts

IoT Integration: Measured by the number of IoT devices (e.g., sensors for asset tracking in transit or oil infrastructure). High device volume expands attack surfaces (Okonkwo, 2021).

Cloud Adoption: Measured by the percentage of processes on cloud platforms (e.g., SaaS ERP). Centralizes data, targeting third-party providers (Adewale, 2022).

Data-Sharing Intensity: Measured by daily data volume exchanged with partners (e.g., contracts, inventory). Heightens risks of interception or middleman attacks.

Automation Penetration: Measured by percentage of automated procurement tasks (e.g., via ERP). Enables post-breach fraudulent transactions (Musa, 2023).

Main Propositions

P1: SCD positively associates with VCR in Nigerian firms.

Sub-Propositions:

P1a: Higher IoT integration increases VCR via network endpoints and device gaps (Okonkwo, 2021).

P1b: Greater cloud adoption raises VCR due to centralized data and third-party reliance (Adewale, 2022).

P1c: More data-sharing intensifies VCR through interception risks.

P1d: Higher automation amplifies VCR by automating breaches (Musa, 2023).

Moderating Factors

P2: Organizational cybersecurity maturity (e.g., training, investments) negatively moderates SCD–VCR link.

P3: Environmental factors (e.g., high cybercrime rates, weak regulations) strengthen it in Nigeria.

Additional influences include human errors (60%+ of breaches; KPMG, 2023), stricter regulations (e.g., GDPR; Trend Micro, 2021), SME vulnerabilities due to limited resources (Borghese, 2023), and power dynamics where dominant firms enforce standards (Li & Wang, 2021).

Contrasting Model Overviews

This review examines five key cyber risk models, critiquing their foundations, applications, and role in enhancing supply chain resilience (SCR), with implications for emerging economies like Nigeria.

FAIR Model

Developed by Jones (2005), FAIR quantifies cyber risk via Loss Event Frequency (Threat Frequency × Vulnerability) and Loss Magnitude (Primary/Secondary). It excels in node-specific financial impacts (e.g., ransomware on suppliers) but struggles with dynamic, network-wide propagation (Freund & Jones, 2014; Böhm et al., 2018).

NIST Cybersecurity Framework (CSF)

NIST's (2018) qualitative framework uses five functions: Identify, Protect, Detect, Respond, Recover. Widely adopted for benchmarking supply chain postures and recovery, it lacks probabilistic modeling of interdependencies (Boyens et al., 2022).

Agent-Based Modeling (ABM)

ABM simulates interactions among agents (firms) to capture emergent behaviors. It models cyber contagion and resilience strategies like dual-sourcing (Ghadge et al., 2019) but requires extensive data and computation.

Bayesian Networks (BN)

BNs use probabilistic graphs for uncertainty and dependencies. Applied to predict incidents from precursors and diagnose root causes in supply chains, they support resilience via control points (Fenz et al., 2014).

Systemic Cyber Risk Models (e.g., CAT)

Adapted from catastrophe modeling, these assess correlated losses using Extreme Value Theory. Ideal for "cyber hurricane" events affecting networks, they inform insurance and macro-risks (Eling & Wirfs, 2019).

Synthesis and Gaps

These models complement each other: FAIR/BNs for node-level diagnosis, NIST for governance, ABM for simulations, and CAT for systemic views. Gaps include siloed applications ignoring cyber attack's unique traits (speed, anonymity) and limited validation in developing economies like Nigeria, where infrastructure differs. Addressing the cyber-supply chain resilience challenge demands moving beyond isolated model application towards an empirically grounded, interdisciplinary synthesis such as Adopting NIST for governance, FAIR/BNs for assets, and ABM for testing. This multi-model synthesis advances cyber-SCR empirically

Empirical Review

Studies in Nigeria show that over 65% of Lagos logistics firms experienced cyber incidents post-digitalization, linked to poor protocols and training (Adebayo & Ojo, 2020; Olumide & Adekunle, 2021). NCC (2023) and NITDA (2022) report rising attacks in pharmaceuticals, agriculture, and retail. Empirical studies consistently demonstrate a positive correlation between the scale of digital technology adoption and exposure to cyber risks. Research by Colicchia et al. (2021) surveying European manufacturers found that each additional digital platform integrated (e.g., ERP, SCM, IoT sensors) increased reported cyber incident frequency by an estimated 18%. Specific vulnerabilities include:

IoT Devices: Often deployed with default passwords and weak encryption, serving as easy entry points (Zhao & Hua, 2020).

Cloud-Based SCM Platforms: Centralized data repositories present high-value targets for ransomware and data breach attacks (He et al., 2022).

Increased Interconnectivity: Digital integration with third-party partners often outpaces the implementation of uniform security protocols, creating "cyber security asymmetries" (Baryannis et al., 2019).

Existing empirical literature on supply chain cybersecurity heavily favors developed economies, leaving emerging markets like Nigeria underexplored. Preliminary Nigerian studies highlight a high-risk environment shaped by several unique factors:

Rapid, uneven digitalization: Firms rush into cloud and mobile SCM tools without adequate cybersecurity investments (Ojebode & Adebayo, 2022).

SME vulnerabilities: small and medium enterprises, central to Nigeria's supply chains, face acute resource shortages for cyber defenses.

Regulatory voids: No tailored legal framework exists beyond the general Nigeria Data Protection Regulation, fostering threats (NITDA, 2023).

Infrastructure woes: Unreliable power and internet disrupt security systems, prompting insecure workarounds.

These challenges indicate a steeper vulnerability trajectory and more arduous cyber-resilience path in Nigeria than global models suggest.

Illustrative Cases

While specific, publicly detailed Nigerian case studies of supply chain cyber-attacks are limited due to companies' reluctance to disclose breaches, international and sectoral examples provide strong conceptual grounding.

Target Data Breach (2013): Hackers gained access to Target's network through a third-party HVAC vendor, compromising 41 million customer records. This case illustrates the risks associated with third-party connections in digitalized supply chains (Krebs, 2014).

NotPetya Ransomware Attack (2017): The NotPetya malware attack on A.P. Moller-Maersk, a global shipping and logistics giant, serves as the ultimate cautionary tale. A malware attack disrupted several global companies, including shipping giant Maersk, highlighting the potential for cyber-attacks to cause significant supply chain disruptions (Greenberg, 2017). As a major global carrier, Maersk's multi-week disruption severely impacted ports and trade worldwide, including Nigerian import/export activities, demonstrating the systemic, global impact of a cyber-attack on a critical supply chain node. This case illustrates the destructive power of malware propagating through a highly digital, interconnected supply chain, leading to billions of dollars in losses.

Colonial Pipeline Ransomware Attack (2021): A ransomware attack on a major fuel pipeline in the United States demonstrated the vulnerability of critical infrastructure to cyber threats, with potential impacts on supply chains (Satter & Polantz, 2021).

Sectoral Case Example: The Nigerian oil and gas sector, with its high-value assets and reliance on SCADA/OT systems, is a primary target. Reports often highlight attempted intrusions targeting pipeline management systems or corporate networks used for logistics and procurement. The increasing use of remote monitoring systems, while efficient, widens the attack surface for sophisticated Advanced Persistent Threats (APTs) seeking intellectual property or disruption. The sector embodies the high-stakes risk of IT/OT convergence, where cyber breach could transition from a financial loss to an environmental or safety disaster.

Empirical Findings

Empirical studies show a clear link between supply chain digitalization and heightened cyber risk vulnerability. For instance, Erevelles et al. (2016) found that highly digitalized firms face greater data breach risks, while Kache and Seuring (2017) noted a positive correlation between big data analytics adoption and cyber-attack susceptibility. Huang et al. (2020) confirmed this trend but emphasized mitigation through cybersecurity investments and training. A growing body of evidence argues that mature, strategic digitalization can enhance cyber resilience. Empirical work by Papanagnou et al. (2022) reveals that advanced digital tools like AI-driven intrusion detection systems and blockchain for secure, immutable transaction ledgers can significantly reduce mean time to detect and recover from attacks. Thus, the relationship is non-linear and contingent: initial and adhoc digital adoption increases vulnerability, while advanced, holistic digitalization with embedded security can mitigate it.

Despite these insights, evidence is limited by fragmented reporting, incomplete risk assessments, organizational unpreparedness, and missing sector-wide standards.

CONCLUSION AND RECOMMENDATIONS

Supply chain digitalization acts as a double-edged sword, delivering benefits like efficiency while heightening cyber risks, with outcomes depending on adoption maturity, strategy, and context. Empirical evidence highlights a key research gap: context-specific, quantitative studies in emerging economies like Nigeria, where

high cloud adoption and data sharing intensify vulnerability to cyber risks (VCR) such as data breaches, downtime, and procurement fraud.

Key Research Gaps and Future Directions

Future empirical studies from institutions like Nasarawa State University Keffi (NSUK) should prioritize:

1. Developing and validating frameworks to assess cyber risk vulnerability in Nigeria's digitally transforming supply chains.
2. Quantifying impacts of technologies like mobile money and local cloud platforms on cyber incidents in agribusiness and manufacturing.
3. Exploring institutional and cultural influences on cybersecurity behaviors among supply chain partners.
4. Adapting models to Nigerian contexts.
5. Developing hybrids (e.g., BN-parameterized ABM).
6. Quantifying human factors like culture and trust.
7. Designing low-cost, scalable resilience models for SME-dominated networks.

These efforts will inform national policy and practices, balancing digitalization's economic growth potential against cyber threats.

Practical Recommendations

To mitigate risks, Nigerian firms should:

1. Implement robust measures like encryption, firewalls, and intrusion detection.
2. Conduct regular risk assessments and security audits.
3. Foster collaboration for sharing best practices.
4. Prioritize cybersecurity in digital strategies, train procurement staff, develop incident response plans, mandate audits for third-party systems, ensure IoT patching, and build SME capacity.
5. Evaluate the Cybercrime Act 2015 for improvements in discouraging attacks.

In conclusion, while digitalization modernizes Nigeria's supply chains, firms must emphasize cyber resilience over rapid adoption to safeguard critical sectors.

REFERENCES

1. African Development Bank. (2020). African economic outlook 2020: Developing Africa’s workforce for the future. AfDB.
2. Adewumi, A., & Oluwaseyi, O. (2022). Cyber security in Nigeria: Trends, challenges and opportunities. Journal of Cyber Security and Information Systems, 1(1), 1–12.
3. Adebayo, O., & Ojo, T. (2020). Cybersecurity challenges in Nigerian logistics supply chains: An empirical investigation. Journal of Supply Chain Management Africa, 12(2), 45–59.
4. Adebayo, V. I., & Ojebode, M. T. (2022). Cybersecurity challenges in Nigeria's emerging digital economy. Nasarawa Journal of Management Sciences.
5. Baryannis, G., et al. (2019). Supply chain risk management and artificial intelligence: State of the art and future research directions. International Journal of Production Research.
6. Böhm, M., Weking, J., & Krcmar, H. (2018). The impact of cybersecurity on supply chain resilience. Proceedings of the 51st Hawaii International Conference on System Sciences.
7. Boyens, J., Paulsen, C., & Bartol, N. (2022). Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. NIST Special Publication 800-161r1.
8. Bostrom, R. P., & Heinen, J. S. (1977). MIS problems and failures: A socio-technical perspective. Management Information Systems Quarterly, 1(3), 17–32.
9. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), 523–548.

10. Büyüközkan, G., & Göçer, F. (2018). Digital supply chain: Literature review and a framework for future research. Computers in Industry, 97, 157–169.
11. Chopra, S., & Meindl, P. (2016). Supply chain management: Strategy, planning, and operation. Pearson.
12. Chopra, S., & Sodhi, M. S. (2014). Managing risk to avoid supply-chain breakdown. MIT Sloan Management Review, 55(1), 53–61.
13. Christopher, M., & Peck, H. (2004). Building the resilient supply chain. International Journal of Logistics Management, 15(2), 1–13.
14. Chui, M., Manyika, J., & Miremadi, M. (2016). Where machines could replace humans—and where they can't (yet). McKinsey Quarterly, (3), 1–13.
15. CISO. (2017). Cyber risk: A primer for boards and audit committees. Chief Information Security Officer (CISO) Magazine.
16. Colicchia, C., et al. (2021). Digitalisation and cyber resilience in supply chains. Production Planning & Control.
17. Erevelles, S., Fukawa, N., & Swayne, L. (2016). Big data and consumer behavior: Imminent opportunities and challenges. Journal of Consumer Marketing, 33(5), 309–316.
18. Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk? Geneva Papers on Risk and Insurance - Issues and Practice, 44(4), 737–766.
19. Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. Information Management & Computer Security, 22(5), 410-430.
20. Freund, J., & Jones, J. (2014). Measuring and Managing Information Risk: A FAIR Approach. Butterworth-Heinemann.
21. Ghadge, A., Weiß, M., Caldwell, N., & Wilding, R. (2019). Managing cyber risk in supply chains: a review and research agenda. Supply Chain Management: An International Journal, 25(2), 223-240.
22. Gartner. (2020). Gartner glossary: Supply chain digitalization.
23. Greenberg, A. (2017). The untold story of NotPetya, the most devastating cyberattack in history. Wired. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
24. He, Y., & Wang, Y. (2021). Cybersecurity risks in digitalized supply chains: A review and research agenda. Supply Chain Management Review, 27(5), 22–34.
25. Huang, X., Wang, X., & Liu, Y. (2020). Supply chain digitalization and cyber risk: A moderated mediation model. International Journal of Production Economics, 229, Article
26. 107746. https://doi.org/10.1016/j.ijpe.2020.107746
27. International Organization for Standardization & International Electrotechnical Commission. (2018). ISO/IEC 27000:2018 information technology—Security techniques—Information security management systems—Overview and vocabulary. https://www.iso.org/standard/73906.html
28. Institute of Risk Management. (2020). Cyber risk: A guide for boards and risk managers. IRM.
29. Ivanov, D., Dolgui, A., & Sokolov, B. (2019). The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics. International Journal of Production Research, 57(3), 829–846.
30. Ivanov, D., Dolgui, A., & Sokolov, B. (2022). The impact of digital technology adoption on supply chain resilience. International Journal of Production Research, 60(3), 695–710.
31. Ivanov, D., et al. (2019). The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics. International Journal of Production Research.
32. Jones, J. (2005). An Introduction to Factor Analysis of Information Risk (FAIR). Risk Management Insight LLC.
33. Kache, F., & Seuring, S. (2017). Challenges and opportunities of digital information at the intersection of Big Data Analytics and supply chain management. International Journal of Operations & Production Management, 37(1), 10–36.
34. Kamalahmadi, M., & Parast, M. M. (2016). A review of the literature on the principles of enterprise and supply chain resilience. International Journal of Production Economics, 171, 116–133. https://doi.org/10.1016/j.ijpe.2015.10.053
35. Krebs, B. (2014, February 5). Target hackers broke in via HVAC company. Krebs on Security. https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/
36. Kshetri, N. (2018). Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications Policy, 42(10), 1027–1038. https://doi.org/10.1016/j.telpol.2018.10.003

37. Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. Decision Support Systems, 51(1), 176–189. https://doi.org/10.1016/j.dss.2010.12.006
38. National Information Technology Development Agency. (2022). Cyber risk trends in Nigerian enterprises.
39. National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.
40. Nigerian Communications Commission. (2022). Cyber security report 2022.
41. Nigerian Communications Commission. (2023). Annual report on cybersecurity incidents in Nigerian supply chains.
42. Oke, A., & Onwuegbuzie, H. (2020). Supply chain digitalization and operational performance: Evidence from Nigerian manufacturing firms. Journal of African Business, 21(4), 523–541. https://doi.org/10.1080/15228916.2019.1705441
43. Olumide, S., & Adekunle, A. (2021). Assessing cyber risk preparedness in Nigerian manufacturing supply chains. African Journal of Information Systems, 13(1), 78–93.
44. Oluwaseyi, O., & Adewumi, A. (2021). Digitalization and cyber security in Nigerian organizations: A review of the literature. International Journal of Cyber Security and Digital Forensics, 10(2), 123–136.
45. Papanagnou, C., et al. (2022). Digital twins for supply chain cyber-resilience: A conceptual framework. Computers & Industrial Engineering.
46. Satter, R., & Polantz, K. (2021, May 13). Colonial Pipeline paid hackers nearly $5 million in ransom. AP News. https://apnews.com/article/colonial-pipeline-hackers-ransome-payments0e0b0a4a4b4b4b4b4b4b4b4b4b4b
47. Tornatzky, L. G., & Fleischer, M. (1990). The processes of technological innovation. Lexington Books.
48. Whitmore, A., Agarwal, A., & Xu, L. D. (2015). The Internet of Things—A survey of topics and trends. Information Systems Frontiers, 17(2), 261–274. https://doi.org/10.1007/s10796-014-9489-3
49. World Bank. (2022). Nigeria digital economy diagnostic report.
50. World Bank. (2023). Doing business in Africa: Regulatory environment and trade facilitation.
51. World Economic Forum. (2023). Global Risks Report 2023.