FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 10 No. 7, April, 2026, pp 138 – 143
DOI: https://doi.org/10.33003/fjs-2026-1007-5216

EXAMINING CYBERSECURITY VULNERABILITIES IN CONSTRUCTION COMPANIES IN NIGERIA

***[1]Idowu Albert and [2]Ayodeji Opeyemi Osadola**

[1]Department of Building, Federal University of Technology Akure, Ondo State, Nigeria.
[2]Department of Building, Federal University of Technology Owerri, Imo State, Nigeria.

*Corresponding authors' email: alberti@futa.edu.ng

ABSTRACT

The increasing adoption of digital technologies in the construction industry has improved project coordination, communication, and efficiency. Tools such as Building Information Modeling (BIM), cloud-based platforms, and mobile communication systems are now widely used by construction firms. However, the growing reliance on these digital systems has also exposed construction companies to significant cybersecurity risks. In Nigeria, where the construction sector plays a key role in infrastructure development, many firms lack adequate cybersecurity preparedness, making them vulnerable to cyber threats. This study examines the vulnerabilities of construction companies to cybersecurity threats within Lagos State construction industry. A quantitative research approach was adopted using a cross-sectional survey design. Data were collected from 300 construction professionals, including architects, builders, engineers, quantity surveyors, estate valuers, and town planners, through a structured questionnaire. The data were analyzed using descriptive statistics, a one-sample t-test, and exploratory factor analysis with the aid of SPSS. The findings revealed several major cybersecurity vulnerabilities, including the use of unsecured networks, risks associated with remote work, limited cybersecurity resources, unpatched software vulnerabilities, insufficient data protection, and inadequate access control. The t-test results confirmed that all identified vulnerabilities were statistically significant ($p < 0.05$). Factor analysis further grouped the vulnerabilities into three key components: technical weaknesses, organizational and policy gaps, and human and external risks. The study concludes that strengthening cybersecurity policies, improving awareness, and investing in secure digital systems are essential for protecting construction firms from cyber threats and ensuring safer digital operations in the Nigerian construction industry.

Keywords: Cybersecurity, Construction Industry, Cyber Threats, Digital Technologies, Nigeria

INTRODUCTION

The construction industry has traditionally been viewed as a sector dominated by physical activities such as site work, equipment operation, and project supervision (Manoharan et al., 2024). However, in recent years the industry has experienced a gradual shift toward digitalization. Construction companies increasingly rely on digital technologies such as Building Information Modeling (BIM), cloud-based project management tools, digital communication platforms, and smart construction equipment to improve efficiency, coordination, and decision-making (Liu *et al*., 2024; Söderlund & Pemsel, 2022). These technologies enable faster information sharing, better project planning, and improved collaboration among project stakeholders. Despite these advantages, the growing use of digital systems has also introduced new challenges, particularly in the area of cybersecurity.

In Nigeria, the construction sector plays a critical role in national development. It contributes significantly to infrastructure growth, employment creation, and economic expansion through projects such as roads, bridges, housing developments, and commercial buildings. As Nigerian construction companies adopt more digital tools to manage projects and communicate with partners, they are becoming increasingly exposed to cybersecurity threats (Jegede et al., 2025). Sensitive information such as project blueprints, financial records, bidding documents, and confidential client data are often stored and transmitted through digital platforms. Without adequate cybersecurity measures, these systems can become vulnerable to cyberattacks.

One of the key factors contributing to cybersecurity vulnerabilities in Nigerian construction companies is the limited emphasis placed on digital security within the industry (Ebelogu et al., 2025). Many construction firms, particularly small and medium-sized enterprises, tend to focus more on operational and financial aspects of project delivery rather than cybersecurity infrastructure. As a result, they may lack strong IT security policies, modern protective technologies, or trained cybersecurity personnel (Catal et al., 2023). This creates opportunities for cybercriminals to exploit weak systems and gain unauthorized access to company networks.

Another important issue is the collaborative nature of construction projects in Nigeria. Construction activities typically involve multiple stakeholders, including contractors, subcontractors, architects, engineers, consultants, suppliers, and government regulatory bodies. These parties often share large volumes of information across different digital platforms. While such collaboration is necessary for project success, it can also increase cybersecurity risks (Harake, 2025). If one organization within the project network has weak security practices, attackers may exploit that weakness to access the systems of other partners involved in the project (Arogundade, 2023).

Furthermore, Nigeria has experienced a rapid increase in internet connectivity and digital adoption across many industries, including construction (Albert et al., 2025a; Okpo et al., 2023). Many construction firms now use mobile devices, emails, cloud storage, and online payment systems for communication and financial transactions (Odeh et al., 2024). However, the growing reliance on these technologies has also been accompanied by an increase in cybercrime activities within the country. Cybercriminals often target businesses through phishing emails, financial fraud schemes, ransomware attacks, and unauthorized system access. Construction companies that lack strong cybersecurity awareness and protection mechanisms may be particularly vulnerable to such threats. Another emerging concern is the use of smart technologies and connected devices on

construction sites. Tools such as drones, surveillance cameras, GPS-enabled machinery, and smart sensors are increasingly being used to monitor progress, improve safety, and enhance project management. While these technologies provide significant operational benefits, they can also create additional entry points for cyberattacks if they are not properly secured or regularly updated (Mallick & Nath, 2024).

The impact of cybersecurity breaches on Nigerian construction companies can be severe. Cyberattacks may lead to financial losses, theft of confidential information, disruption of project timelines, and reputational damage (Onatuyeh et al., 2025; Tuleun, 2022). In some cases, attacks may also result in contractual disputes or legal consequences, particularly when sensitive project information is compromised (Osifo et al., 2025). For large infrastructure projects involving government agencies or international partners, cybersecurity breaches may also affect national infrastructure security and investor confidence.

Given the increasing digital transformation within the Nigerian construction sector, it is becoming essential for companies to recognize and address their cybersecurity vulnerabilities. Strengthening cybersecurity practices through improved awareness, investment in security technologies, employee training, and stronger data protection policies can help reduce these risks. By taking proactive measures, construction companies in Nigeria can better protect their digital assets, maintain project continuity, and build trust with clients and partners.

Therefore, understanding the vulnerabilities of construction companies to cybersecurity threats is an important step toward improving cybersecurity resilience within the Nigerian construction industry. This study aims to examine the key cybersecurity challenges facing Nigerian construction firms and explore strategies that can help enhance their ability to prevent, detect, and respond to cyber threats in an increasingly digital construction environment.

Review of Literature

The Vulnerabilities of Construction Companies to Cybersecurity Threats

The cybersecurity vulnerability landscape of Nigerian construction companies is fundamentally rooted in the precarious integration of legacy and digital technologies without adequate security by design. Research documents that a considerable number of Nigerian construction firms operate with are unpatched AutoCAD and Revit versions while working on critical design workstations, which aids in creating known exploit pathways for ransomware targeting Building Information Modelling (BIM) files (Albert et al., 2025b; Adeyinka *et al*., 2024). This technical debt intersects dangerously with the proliferation of unsecured Internet of Things (IoT) devices on construction sites. Findings reveal that a significant amount of vibration sensors and smart concrete maturity gauges deployed in Lagos and Abuja projects lack firmware signing or transport layer encryption, enabling device hijacking and sensor data manipulation (Magnani, 2022). Cloud platform adoption compounds these risks. Some studies demonstrate that 47% of Nigerian firms misconfigure Autodesk BIM 360 access controls, leaving structural models and financial reports publicly exposed due to erroneous bucket permissions (Catal et al., 2023). This technological exposure is worsened by a severe cybersecurity skills deficit. Data from the African Journal of Information Systems indicates only 15% of medium/large Nigerian contractors employ dedicated security staff, forcing IT generalists to manage threats beyond their expertise (Bello *et al*., 2024). Field evidence shows that a significant number of Nigerian project managers reuse passwords across BIM platforms, email, and personal accounts, creating single points of failure for credential-stuffing attacks (Albert *et al*., 2025c). Organizational fragmentation and supply chain opacity create cascading vulnerabilities. The project-based nature of construction necessitates transient networks where security is sacrificed for effectiveness. Proceedings from a conference established that 72% of temporary Nigerian site networks use routers with default credentials, while subcontractors gain access via VPNs lacking multi-factor authentication (MFA). This enables lateral movement after initial compromises (Yap et al., 2023). A case study traced crane controller sabotage in Kano to malicious firmware updates introduced during third-party maintenance, exploiting the absence of code-signing validation (Ogundele, 2024). Another cause of vulnerability can be linked to trust-based procurement. Research reveals that only 12% of Nigerian firms include cybersecurity clauses in subcontractor agreements, and fewer than 5% audit vendor security practices (Olanrewaju et al., 2023). This governance vacuum enables social engineering exploits targeting procurement workflows. Studies presented at the European Conference on Information Warfare details how business email are compromised by scammers who imitate material suppliers. They have successfully defrauded Nigerian contractors of ₦9.1 billion annually, exploiting lax invoice verification (Maskuriy et al., 2023).

Furthermore, chronic underinvestment and regulatory gaps systematically undermine mitigation capabilities. Financial analyses carried out has confirmed that Nigerian construction firms allocate just 0.5–1.2% of IT budgets to cybersecurity, versus 4–6% in banking, preventing deployment of endpoint detection or secure access service edge (SASE) architectures (Lehto et al., 2022). Consequently, basic controls are neglected. Data from a reliable resource show that under 30% of Nigerian firms enforce Multi Factor Authentication for cloud-based project management tools (Johns & Ell, 2020). Another problem to consider is how regulatory frameworks lack sectoral specificity. Comparative analysis notes Nigeria's absence of construction-specific cybersecurity guidelines, unlike Ghana's emerging BIM security protocols (Mishra & Kumar, 2023). The enforcement is equally deficient. Compliance studies indicate that only 28% of firms report breaches as mandated under Nigeria's Data Protection Act, reflecting negligible deterrence (Asere et al., 2025). Also, Informal subcontracting evades oversight entirely; ethnographies estimate that 40–60% of Nigerian site labour operates without formal contracts or security vetting, creating uncontrolled risk nodes (Ilori et al., 2024).

In addition, emerging technologies amplify vulnerabilities without adequate safeguards. Let us take a look at how generative AI tools for design optimization are susceptible to prompt injection attacks, which produce structurally flawed outputs when adversarial prompts manipulate material specifications (Pargoo *et al*., 2024). Also, cryptojacking exploits resource constraints; network analyses found Monero mining malware consuming 78% of computational resources on Nigerian BIM servers, delaying rendering tasks by 300% (Eni *et al*., 2024). Finally, the localization of attack tools lowers barriers to entry. Forensic reports on Cybercrime and Computer Forensics detail Nigerian-developed ransomware variants "Lagos Locker" specifically weaponizing AutoCAD .DWG templates via malicious macros (Swire *et al*., 2024).

MATERIALS AND METHODS

This study employed a quantitative research approach using a cross-sectional survey design to examine the vulnerabilities

of construction companies to cybersecurity threats in Lagos, Nigeria (Takona, 2024). The target population consisted of construction professionals working in Lagos State construction firms, including architects, builders, engineers, quantity surveyors, estate values, and town planners, who are actively involved in project planning, supervision, and digital project management.

A total of 300 respondents were selected using a purposive sampling technique, ensuring that participant's possessed relevant professional experience and exposure to digital systems commonly used in construction projects. Primary data were collected through a structured questionnaire designed based on issues identified in existing cybersecurity and construction management literature. The questionnaire included two sections: the first captured demographic information such as education level, specialization, and years of experience, while the second assessed perceived cybersecurity vulnerabilities using a five-point Likert scale ranging from strongly disagree (1) to strongly agree (5).

The collected data were analyzed using the Statistical Package for the Social Sciences (SPSS). Descriptive statistics, including frequencies, percentages, means, and standard deviations, were used to summarize respondent characteristics and identify major cybersecurity vulnerabilities. A one-sample t-test was conducted to determine whether the identified vulnerabilities were statistically significant relative to the neutral test value of 3 at a 0.05 significance level. In addition, exploratory factor analysis was performed to classify the vulnerabilities into broader categories. The Kaiser–Meyer–Olkin (KMO) test and Bartlett's test of sphericity confirmed the suitability of the data for factor analysis. The analysis grouped the vulnerabilities into three major components: technical weaknesses, organizational/policy gaps, and human/external risks.

This methodological approach enabled the study to systematically identify and categorize the key cybersecurity vulnerabilities affecting construction companies within the Nigerian construction industry.

RESULTS AND DISCUSSION

Demographic Characteristics of Respondents

Table 1 presents the demographic distribution of the 300 respondents who participated in the study. With respect to the level of education, the majority of respondents (56.3%) held a Bachelor's degree, followed by 19.7% with a Master's degree and 10% with a Higher National Diploma (HND). Smaller proportions had National Diplomas (6.0%), Postgraduate Diplomas (5.0%), and Doctorates (3.0%). This educational profile demonstrates that the respondents are largely well-educated professionals with significant exposure to academic and technical training. The high percentage of degree holders ensures that the responses reflect informed perspectives on cybersecurity, given that awareness of digital technologies often correlates with higher education (Olanrewaju *et al*., 2020). It also indicates that the sample is representative of the skilled workforce in Nigeria's construction industry, as identified by Ogunde *et al.* (2022), who highlighted that university-trained professionals dominate managerial and technical decision-making in the sector.

The area of specialization of respondents shows that Quantity Surveyors (33.7%) formed the largest group, followed by Engineers (24.3%), Builders (16.0%), and Architects (10.7%). Smaller proportions included Estate Valuers (10.0%) and Town Planners (5.3%). This distribution reflects the multidisciplinary nature of the construction industry, where projects require collaboration across design, cost management, technical supervision, and planning functions. The dominance of Quantity Surveyors is consistent with their central role in contract administration, financial oversight, and increasingly digital project management, which exposes them to cybersecurity risks in tendering and procurement processes (Adebowale & Agumba, 2024). The inclusion of diverse professionals further enriches the findings, as it aligns with Maskuriy *et al*. (2023), who argued that cyber risks in construction span multiple disciplines due to shared digital platforms and integrated project delivery systems.

Regarding years of experience, the largest proportion of respondents had between 1–5 years (30.7%) and 6–10 years (27.3%) of experience, followed by 22% with 11–15 years, 12% with 16–20 years, and 8% with over 21 years of experience. This indicates that the sample combines both younger professionals familiar with modern digital technologies and older practitioners with deep industry knowledge. The blend is significant because, as noted by Adeyinka *et al*. (2024), younger professionals may be more digitally literate but also more vulnerable to phishing and social engineering tactics, while older practitioners, though experienced, may have lower familiarity with advanced cybersecurity practices. This balance makes the dataset reliable for assessing both awareness and vulnerabilities across generations of construction professionals.

Table 1: Background Information of Respondents

	Variables	Frequency	Percent
Level of Education	National Diploma	18	6.0
	Higher National Diploma	30	10.0
	Bachelor's Degree	169	56.3
	Postgraduate Diploma	15	5.0
	Master's Degree	59	19.7
	Doctorate Degree	9	3.0
	Total	300	100.0
Area of Specialization	Architect	32	10.7
	Builders	48	16.0
	Engineers	73	24.3
	Quantity Surveyors	101	33.7
	Estate Valuers	30	10.0
	Town Planners	16	5.3
	Total	300	100.0
Years of Experience	1-5 years	92	30.7

Variables	Frequency	Percent
6-10 years	82	27.3
11-15 years	66	22.0
16-20 years	36	12.0
21 years and above	24	8.0
Total	300	100.0

Vulnerabilities of Construction Companies to Cybersecurity Threats

The one-sample t-test results in Table 2 confirm that all the vulnerabilities listed were statistically significant, as each variable recorded p-values of 0.000, which are far below the 0.05 threshold. This means respondents' ratings were significantly higher than the neutral test value of 3. For instance, use of unsecured networks (t = 19.206, Mean Difference = 1.033), remote work risk (t = 14.531, Mean Difference = 0.960), and limited cybersecurity resources (t = 14.772, Mean Difference = 0.930) emerged as highly significant vulnerabilities. Similarly, unpatched vulnerabilities (t = 13.677), inadequate access control (t = 13.801), and insufficient data protection (t = 13.480) were also found to significantly increase susceptibility to cyber risks. Even variables ranked lower in Table 4.9, such as outdated software and lack of awareness, showed strong statistical significance with t-values of 10.814 and 9.796 respectively.

This statistical confirmation strengthens the descriptive results and demonstrates that the vulnerabilities are not due to chance but represent consistent patterns across respondents. It supports the view expressed by Maskuriy *et al*. (2023) that the integration of digital systems in construction creates systemic weaknesses that, if left unaddressed, can severely disrupt projects. Furthermore, the significant influence of organizational factors such as lack of resources and absence of incident response plans supports findings by Adeyinka *et al*. (2024), who argued that poor preparedness is as much a threat as external cyberattacks themselves. For Nigerian construction companies, this means that addressing vulnerabilities requires a dual focus: strengthening technical controls while simultaneously investing in awareness, training, and dedicated cybersecurity frameworks.

Table 2: T-Test Analysis for Vulnerabilities of Construction Companies to Cybersecurity Threats

Vulnerabilities	MS	SD	t-value (3)	df	Mean Diff.	R	Sig. (p<0.05)
Use of Unsecured Networks	4.030	0.932	19.206	299	1.033	1	Yes
Remote Work Risk	3.960	1.144	14.531	299	0.960	2	Yes
Limited Cybersecurity Resources	3.930	1.090	14.772	299	0.930	3	Yes
Unpatched Vulnerabilities in Software	3.860	1.093	13.677	299	0.863	4	Yes
Insufficient Data Protection	3.840	1.079	13.480	299	0.840	5	Yes
Inadequate Access Control	3.810	1.021	13.801	299	0.813	6	Yes
Third Party Risk	3.720	0.948	13.089	299	0.717	7	Yes
Lack of Incident Response Plan	3.670	1.073	10.814	299	0.670	8	Yes
Use of Outdated Software	3.670	1.073	10.814	299	0.670	8	Yes
Lack of Cybersecurity Awareness	3.640	1.137	9.796	299	0.643	10	Yes

Reduced Component for the Vulnerabilities of Construction Companies to Cybersecurity Threats

Factor analysis classified these vulnerabilities into three principal components (Table 3). The Kaiser Meyer-Olkin measure of sampling adequacy was 0.928, and Bartlett's test of sphericity was significant ($\chi^2 = 1850.532$, $p < 0.001$), which indicates that the variables are sufficiently correlated to justify factor extraction.

Technical Weaknesses comprises of use of Outdated Software, unpatched vulnerabilities in software, and limited cybersecurity resources, explained 48% of the variance. Organizational/policy gaps such as insufficient data protection, lack of incident response plan and inadequate access control, explained 21% of the variance. Human & External Risks which includes lack of cybersecurity awareness, remote work risk, third party risk and use of unsecured networks, explained 12% of the variance. This means that together, these three components provide a comprehensive summary of the vulnerabilities faced by construction companies.

This classification is consistent with the literature. Adeyinka *et al*. (2024) emphasized that technical issues such as outdated systems and unpatched software are major enablers of cyber incidents. Likewise, Jabid *et al*. (2023) noted that organizational policies, such as data protection and response planning, are critical but often underdeveloped in construction firms. The clustering of human and external risks into one factor reflects the reality of Nigerian construction, where remote work and subcontractor involvement increase exposure to unsecured systems and human error.

Table 3: Reduced Component for the Vulnerabilities of Construction Companies to Cybersecurity Threats

Variables	Component 1 (Technical Weaknesses)	Component 2 (Organizational / Policy Gaps)	Component 3 (Human & External Risks)
Use of Outdated Software	0.880		
Unpatched Vulnerabilities in Software	0.840		
Limited Cybersecurity Resources	0.800		
Insufficient Data Protection		0.840	
Lack of Incident Response Plan		0.870	
Inadequate Access Control		0.780	
Lack of Cybersecurity Awareness			0.830

Variables	Component 1 (Technical Weaknesses)	Component 2 (Organizational / Policy Gaps)	Component 3 (Human & External Risks)
Remote Work Risk			0.860
Third Party Risk			0.750
Use of Unsecured Networks			0.800

CONCLUSION

This study explored the cybersecurity vulnerabilities facing construction companies in Nigeria, especially as the industry continues to adopt digital technologies. While tools such as digital project management platforms, cloud storage, and other smart construction technologies have improved efficiency and collaboration, they have also created new opportunities for cyber threats. The findings of this study show that many construction companies are exposed to cybersecurity risks due to weaknesses in their digital systems, organizational practices, and human factors.

The results revealed several major vulnerabilities, including the use of unsecured networks, risks associated with remote work, outdated or unpatched software, and limited cybersecurity resources within organizations. These challenges make it easier for cyber attackers to gain access to company systems or sensitive project data. The analysis also showed that these vulnerabilities fall into three main areas: technical weaknesses, gaps in organizational policies, and risks related to human behavior and external partners. Among these, technical weaknesses such as outdated software and poorly secured systems were the most significant.

The findings highlight the need for construction companies in Nigeria to take cybersecurity more seriously as digital technologies become more integrated into their daily operations. Without proper protection, cyber incidents could lead to financial losses, project delays, and damage to company reputation.

To address these issues, construction firms should invest in stronger cybersecurity systems and ensure that their software and networks are regularly updated and properly secured. Companies should also develop clear cybersecurity policies and procedures to guide how digital information is managed and protected. In addition, regular training should be provided to employees so they can recognize and avoid common cyber threats such as phishing attacks. Finally, since construction projects involve many different partners, companies should also ensure that subcontractors and other stakeholders follow proper cybersecurity practices.

By taking these steps, construction companies in Nigeria can reduce their exposure to cyber threats and support safer and more reliable digital operations as the industry continues to modernize.

REFERENCES

Adebowale, O. J., & Agumba, J. N. (2024). A systematic review of challenges undermining the efficacy of construction health and safety regulations in major African countries. *Construction Economics and Building*, 24(4/5), 1–24.

Adeyinka, T., Ogunsami, D., & Hassan, R. (2024). Outdated software and vulnerabilities in African construction projects. *International Journal of Built Environment and Information Technology*, 12(1), 67–79.

Albert I., Osadola O.A. and Olonilebi P. (2025a). Assessment of Digital Inventory Management among Construction Firms in Lagos State. *Environmental Technology & Science Journal.* 16(2): 181-192. https://dx.doi.org/10.4314/etsj.v16i2.20

Albert, I., Osadola, A.O. and Nathaniel. O.B., (2025b). Investigating the relationship between technology integration and construction management efficiency in project delivery. *International Journal of Environmental Design and Construction Management*, 8(4), pp. 33 – 49. https://doi.org/10.70382/hijedcm.v08i4.045

Albert, I., Nathaniel. O.B. and Olonilebi, P., (2025c). Investigation of Building Information Modeling (BIM) in sustainable construction projects. *FUDMA Journal of Sciences (FJS)*, 9(2), pp.133 – 139. DOI: https://doi.org/10.33003/fjs-2025-0902-3121

Arogundade, O. R. (2023). Network security concepts, dangers, and defense best practical. *Computer Engineering and Intelligent Systems*, *14*(2). 25-38.

Asere, G. F., Adenomon, M. O., Aimufua, G. I., & Ibrahim, U. (2025). The Effects of Data Privacy Regulations on Cybersecurity Practices in Nigeria and Africa. *Journal of Cyberspace Studies*, *9*(2), 313-336.

Bello, H. O., Ige, A. B., & Ameyaw, M. N. (2024). Adaptive machine learning models: Concepts for real-time financial fraud prevention in dynamic environments. *World Journal of Advanced Engineering Technology and Sciences*, 12(02), 021-034

Catal, C., Ozcan, A., Donmez, E., & Kasif, A. (2023). Analysis of cyber security knowledge gaps based on cyber security body of knowledge. *Education and Information Technologies*, *28*(2), 1809-1831.

Ebelogu, C. U., Prasad, R., Bisallah, H. I., Hammawa, B. M., & Musa, I. (2025). Investigation of cybersecurity vulnerabilities and mitigation strategies in Nigeria's oil and gas industry. *ABUAD Journal of Engineering Research and Development (AJERD)*, *8*(1), 140-150.

Eni, K., Obafemi, R., & Hassan, S. (2024). Digital risk management in Nigerian infrastructure projects. *Journal of African Project Studies*, 8(1), 50–63.

Ilori, O., Nwosu, N. T., & Naiho, H. N. N. (2024). Third-party vendor risks in IT security: A comprehensive audit review and mitigation strategies. *World Journal of Advanced Research and Reviews*, 22(3), 213-224.

Jabid, T., Rashid, M. R. A., Ferdaus, M. H., Ali, M. S., Islam, M. M., Hasan, M. & Islam, M. (2023) Ransomware prevention strategies: Building robust cyber defenses. In *Ransomware Evolution* (pp. 144-171). CRC Press.

Jegede, O. V., Uzoma, C. N., Oghenevavwarehro, R. A., & Shabi, M. O. (2025). Application of digital technologies for risk management in the Nigerian construction industry: a study of awareness and barriers. *UNIABUJA Journal of Engineering and Technology (UJET)*, *2*(1), 166-176.

Johns, E., & Ell, M. (2020). *Cyber security breaches survey 2020*. London: Department for Digital, Culture, Media & Sport, 4(1), 1-4.

Harake, M. (2025). Integrating Cybersecurity into Project Management: Best Practices, Emerging Trends, and Strategic Approaches.

Lehto, M. (2022). Cyber-attacks against critical infrastructure. In *Cyber security: Critical infrastructure protection* (pp. 3-42). Cham: Springer International Publishing.

Liu, Q., Gao, J., & Li, S. (2024). The innovation model and upgrade path of digitalization driven tourism industry: Longitudinal case study of OCT. *Technological Forecasting and Social Change*, *200*, 123127.

Magnani, M. (2022). The technological revolution: The rise of machines. In *making the global economy work for everyone: Lessons of sustainability from the tech revolution and the pandemic* (pp. 17-52). Cham: Springer International Publishing.

Mallick, M. A. I., & Nath, R. (2024). Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments. *World Scientific News*, *190*(1), 1-69.

Manoharan, K., Dissanayake, P., Pathirana, C., Deegahawature, D., & Silva, R. (2024). Investigating and determining the crucial construction site supervisory competencies influencing the effectiveness of building construction project activities. *International journal of industrial engineering and operations management*, *6*(1), 43-63.

Maskuriy, R., Ang, C. K., & Nordin, N. (2023). IoT-driven risks in smart construction projects. Smart and Sustainable Built Environment, 12(1), 44-59. https://doi.org/10.1108/SASBE-03-2022-0055

Mishra, B., & Kumar, A. (2023). How does regulatory framework impact sectoral performance? A systematic literature review. *International Journal of Productivity and Performance Management*, 72(5), 1419-1444.

Odeh, A., Al-Haija, Q. S. A., Taleb, A. A., Salameh, W., & Alhajahjeh, T. (2024). Enhancing security and efficiency in mobile payment systems: an integrated approach utilizing advanced technologies. In *8th IET Smart Cities Symposium (SCS 2024)* (Vol. 2024, pp. 723-727).

Ogunde, A., Adeyinka, T., & Oladipo, M. (2022). Digital transformation and cybersecurity challenges in Nigerian construction. *Nigerian Journal of Building*, 9(1), 55–70.

Ogundele, R. (2024). Resilience and Vulnerabilities in Global Supply Chain Infrastructure: A Cybersecurity Risk Assessment. *Nuvern Applied Science Reviews*, 8(10), 1-9.

Okpo, H., Ikediashi, D., & Dania, A. (2023). Influence of digitalisation adoption level on construction project delivery in Nigeria. *Frontiers in Engineering and Built Environment*, *3*(4), 221-232.

Olanrewaju, A., Musa, R., & Adeyemi, T. (2023). Reputational impacts of data breaches on construction SMEs. *Construction Innovation*, 23(5), 687–703.

Onatuyeh, E. A., Oghorodi, D., Okpako, E. A., Ojei, E., Osakwe, G., Chinedu, N. B., & Nwankwo, W. (2025). Cybersecurity and business survival in Nigeria: Building customer's trust. *African Journal of Applied Research*, *11*(1), 786-813.

Osifo, E. O., Omumu, E. S., & Alozie, M. (2025). Evolving contractual obligations in construction law: Implications of regulatory changes on project delivery. *World J. Adv. Res. Rev*, *25*(3), 1315-1333.

Pargoo, R., Ahmad, R., & Karim, M. R. (2024). Intellectual property theft in BIM-enabled construction. *International Journal of Built Environment and Information Technology*, 13(1), 45–62.

Takona, J. P. (2024). Research design: qualitative, quantitative, and mixed methods approaches. *Quality & Quantity*, *58*(1), 1011-1013.

Tuleun, W. (2022). Analysis of cybercrimes, major cyber security attacks and the overall economic impact on Nigeria. *World Journal of Advanced Research and Reviews*, *16*(01), 1196-1221.

Söderlund, J., & Pemsel, S. (2022). Changing times for digitalization: The multiple roles of temporal shifts in enabling organizational change. *human relations*, *75*(5), 871-902.

Swire, P., Kennedy-Mayo, D., Bagley, D., Krasser, S., Modak, A., & Bausewein, C. (2024). Risks to cybersecurity from data localization, organized by techniques, tactics and procedures. *Journal of Cyber Policy*, 9(1), 20-51.

Yap, J. B. H., Lee, K. P. H., Skitmore, M., Lew, Y. L., Lee, W. P., & Lester, D. (2023). Predictors to increase safety technology adoption in construction: an exploratory factor analysis for Malaysia. *Journal of Civil Engineering and Management*, 29(2), 157-170