Asian Journal of Engineering and Applied Technology
ISSN: 2249-068X (P); 3049-1959 (E)
Vol.14 No.1, 2025, pp.33-38

www.crijournals.org
DOI: https://doi.org/10.70112/ajeat-2024.14.1.4297

A Sectoral Study of Cyber Threats and Vulnerability Management in Resource-Constrained Nigerian SMEs'

Aminu Muhammad Auwal[1*] and James Olaoluwa Abiodun[2]
[1*]Faculty of Natural Sciences, University of Jos, Plateau State, Nigeria
[2]Department of Computer Science, Federal Polytechnic Bida, Bida, Niger State, Nigeria
Email: olaoluwajames1@gmail.com
*Corresponding Author: i.elameenu@gmail.com
(Received 5 March 2025; Revised 20 March 2025; Accepted 15 April 2025; Available online 20 April 2025)

***Abstract* - Nigerian SMEs face increasing cyber threats due to unpatched vulnerabilities and limited cybersecurity resources. Human and technical constraints have contributed to weak defences, exposing businesses to malware, ransomware, and social engineering attacks. Understanding these risks is essential to improving cybersecurity resilience. This study investigates the prevalence and severity of unpatched vulnerabilities among 100 Nigerian SMEs, focusing on how human and technical constraints influence their cybersecurity posture. An anonymous web-based survey was used to assess patch management practices, exposure to cyber threats, and security gaps. Responses were analyzed thematically to identify recurring patterns of weakness in human behavior, technical infrastructure, and organizational practices. Findings reveal that 78% of SMEs experienced at least one cybersecurity incident in the past year. The most common threats were social engineering (42%) and unpatched software vulnerabilities (38%). Thematic analysis of 65 qualitative responses identified key challenges such as ineffective security practices (n=25), low cybersecurity awareness (n=22), and resource constraints (n=18). Notably, only 29% of SMEs had a dedicated cybersecurity budget. These findings highlight the urgent need for sector-specific, cost-effective training and affordable security frameworks tailored to SMEs. Practical policy support is essential to bridging the cybersecurity gap in resource-constrained environments.**
Keywords: **Cybersecurity Resilience, Unpatched Vulnerabilities, Small and Medium Enterprises (SMEs), Social Engineering, Human and Technical Constraints**

I. INTRODUCTION

Nigerian SMEs are increasingly facing significant cybersecurity threats, which pose substantial risks to their operations and growth. Studies indicate that SMEs are particularly vulnerable to cyber threats such as phishing, malware, and ransomware due to resource constraints and inadequate cybersecurity measures [1]. These cyberattacks can lead to severe financial losses, data breaches, and operational disruptions, ultimately undermining the stability and trust in these enterprises [2]. A common misconception is that SMEs are not primary targets for cybercriminals; however, recent findings reveal that their lack of robust cybersecurity measures makes them attractive targets [1]. Emerging research highlights the growing vulnerability of SMEs and emphasizes the urgent need for comprehensive cybersecurity policies and regular employee training to mitigate risks [1]. A key concept in cybersecurity is "unpatched vulnerabilities," referring to security flaws in software or systems that have not been addressed, leaving them open to exploitation. Another critical concept is "social engineering," which involves manipulating individuals into disclosing confidential information, often through deceptive emails or messages [1]. Both human and technical constraints-such as limited cybersecurity awareness, insufficient technological infrastructure, and resource limitations-contribute significantly to the cybersecurity challenges faced by Nigerian SMEs [2], [3]. The National Cybersecurity Policy and Strategy (NCPS) is a major initiative by the Nigerian government aimed at strengthening the country's cybersecurity framework [4]. This policy plays a vital role in supporting SMEs by providing guidelines and strategies to protect their digital assets and ensure business continuity in the face of cyber threats [2], [4]. However, significant gaps remain in compliance and awareness. Many SMEs continue to struggle with implementing effective cybersecurity measures, leading to persistent vulnerabilities and losses from cyberattacks [2], [4]. This research contributes to enhancing cybersecurity resilience among Nigerian SMEs by identifying these gaps and recommending actionable strategies to improve compliance and awareness, thereby strengthening their overall cybersecurity posture [2], [4].

II. OBJECTIVES OF THE STUDY

This study aims to investigate the prevalence and severity of unpatched software vulnerabilities in Nigerian SMEs, with a particular focus on the role of human and technical constraints in shaping cybersecurity risks. Using an anonymous web-based survey of 100 SMEs across various industries, the research seeks to identify common security gaps, assess exposure to social engineering attacks and infrastructure weaknesses, and evaluate the level of cybersecurity awareness and investment among SME stakeholders. The findings are intended to inform the development of sector-specific, cost-effective cybersecurity interventions that are practical and scalable for resource-constrained enterprises.

III. METHODOLOGY

A. Design

This study employed a cross-sectional research design using an anonymous, web-based survey to collect both quantitative and qualitative data from 100 government-registered Small and Medium Enterprises (SMEs) operating across diverse sectors in Nigeria. The design was selected to facilitate broad participation and enable the exploration of cybersecurity practices, experiences, and perceptions within a real-world organizational context.

1. Sampling and Recruitment: Participants were selected using a randomized sampling technique to ensure diversity across sectors and organizational types. SMEs in this study are defined as enterprises with fewer than 250 employees and limited annual turnover, consistent with recognized local classifications. In the absence of centralized online directories or formal SME associations in the study area, eligible SMEs and SME-like institutions were identified through local networks, informal referrals, and direct outreach to small business owners, private institutions, and commercial operators. The study also included organizations such as private secondary schools and other small- to medium-sized service providers that operate within the SME category in terms of size and structure. Efforts were made to ensure balanced representation across retail, education, services, ICT, and other relevant sectors. To maintain data relevance and accuracy, participation was limited to individuals in decision-making roles such as business owners, managers, or IT staff with knowledge of their organization's cybersecurity practices.

2. Instrument Development: The survey instrument comprised 32 structured and semi-structured questions designed to capture multiple dimensions of cybersecurity readiness. Quantitative items measured the prevalence of cyber incidents, the frequency and types of threats encountered, and the extent of cybersecurity budgeting and infrastructure in place. These questions enabled statistical analysis of trends in patch management, threat exposure, and security resource allocation.

The qualitative component included open-ended prompts that allowed participants to describe specific cybersecurity challenges and vulnerabilities faced by their organizations. These narrative responses offered rich contextual data to complement and deepen the quantitative findings.

The survey was designed to investigate key thematic areas: (1) the status of software update and patching practices; (2) the nature and frequency of cyber threats such as phishing, ransomware, and data breaches; (3) internal cybersecurity policies and employee behavior; (4) levels of awareness and investment in cybersecurity measures; and (5) the availability and quality of technical infrastructure and training. The questionnaire was pilot-tested with 5 SMEs to ensure clarity and relevance, and feedback was used to refine the instrument prior to full deployment.

3. Data Collection Procedure: The data collection was conducted online over a four-week period using a secure digital platform. Participants received a survey link via email and social media channels. Prior to completing the questionnaire, each participant was presented with a brief description of the study, its purpose, and their rights as respondents. Participation was voluntary, and informed consent was obtained digitally. To maintain anonymity, no personally identifiable information was collected. Out of 120 SMEs invited, 100 completed the survey, yielding a response rate of 83.3%.

4. Data Analysis: Quantitative data were analyzed using descriptive statistics to summarize frequencies, percentages, and key trends across SMEs. These results provided insight into the scale and distribution of cybersecurity issues such as patching delays, exposure to cyber threats, and security investment levels.

For qualitative analysis, 65 usable open-text responses were examined using thematic analysis, following Braun and Clarke's (2006) six-step framework. Initial coding was used to identify key concepts, which were then grouped into broader themes related to human behavior, organizational policy, technical limitations, and vendor reliance. A total of 12 responses were excluded due to lack of relevant content or incomplete information. To minimize researcher bias during thematic analysis, codes and themes were reviewed by an independent colleague for consistency.

5. Ethical Considerations: All ethical protocols were strictly followed. The study guaranteed participants' anonymity, ensured data confidentiality, and informed respondents of their right to withdraw at any point without consequence. Data were stored securely and used solely for the purpose of academic research.

B. Results

A total of 100 SMEs participated in the survey, with 78% reporting at least one cybersecurity incident in the past year. The study collected both quantitative and qualitative data to assess the cybersecurity challenges faced by SMEs. The quantitative data focused on the frequency and nature of cyber threats, as well as the availability of security resources, while the qualitative responses (n = 65) provided deeper insights into the underlying causes of security gaps. A thematic analysis was conducted on the open-ended responses, identifying key areas of concern.

Twelve responses were excluded due to irrelevance or insufficient detail, resulting in 53 responses for qualitative analysis. A word cloud was generated (Figure 1), and a trend analysis of key cybersecurity terms was performed (Figure 2). The findings are presented in two sections: quantitative results, followed by qualitative insights.

C. Quantitative Findings

1. Cybersecurity Incidents:
2. 78% of SMEs reported experiencing at least one cyberattack in the past year.
3. Most Common Threats:
   a) Social engineering and impersonation scams – 42%
   b) Unpatched software vulnerabilities – 38%
   c) Ransomware and malware infections – 23%
4. Cybersecurity Resources:
   a) SMEs with a dedicated cybersecurity budget – 29%
   b) SMEs relying solely on free security tools – 54%
   c) SMEs conducting regular employee cybersecurity training – 18%

D. Unpatched Software and Outdated Systems (n=22)

Many SMEs reported using outdated software and failing to apply security patches, leaving their systems vulnerable to cyber threats. Respondents identified cost constraints and a lack of technical knowledge as the primary barriers to maintaining up-to-date systems. One participant noted, "Most of our systems run on outdated software because upgrading is too expensive for small businesses like ours."

E. Phishing and Business Email Compromise (n=18)

Phishing and email scams emerged as major security threats, with employees frequently falling victim due to insufficient awareness and training. Many SMEs reported lacking advanced email security solutions. One respondent stated, "We receive phishing emails almost every week, and sometimes staff unknowingly click on malicious links, exposing our systems."

Fig. 1 Word Cloud Generated from Qualitative Responses, Highlighting Key Cybersecurity Concerns

Fig. 2 Trends Analysis of Key Cybersecurity Terms Across Qualitative Responses. The Graph Illustrates the Relative Frequency of Selected Terms Across Different Document Segments, Highlighting Patterns in Cybersecurity Concerns Among SMEs.

F. Limited IT Security Resources (n=15)

A significant number of SMEs reported lacking dedicated IT staff or formal cybersecurity measures, making them vulnerable targets for cybercriminals. Respondents expressed concerns regarding the affordability of cybersecurity solutions. One participant noted, "As a small business, we cannot afford a cybersecurity expert, so we rely on basic antivirus software, which is not sufficient."

G. Weak Password and Access Control Practices (n=10)

Poor password management and weak access control policies were frequently cited as significant security risks. Many SMEs reported relying on shared passwords or reusing credentials across multiple accounts. One respondent stated, "We still use shared passwords for most of our accounts because it is easier for employees to log in, but we know it is risky."

H. Lack of Cybersecurity Awareness and Training (n=8)

Many SMEs acknowledged that their employees had little to no cybersecurity training, increasing their susceptibility to social engineering attacks. The cost of training was frequently cited as a major barrier. One respondent remarked,

"Most of my staff do not understand cybersecurity risks, and training them costs money we do not have."

I. Reliance on Third-Party Services (n=6)

Some SMEs reported relying on external IT service providers but expressed concerns regarding the adequacy of the security measures implemented by these vendors. One respondent stated, "We outsource our IT security, but we do not really know if they are following the best cybersecurity practices."

J. Cyber Insurance and Compliance Concerns (n=5)

A small percentage of respondents considered cyber insurance and regulatory compliance as factors influencing their cybersecurity strategy. However, many found compliance requirements confusing or difficult to implement. One participant noted, "We looked into cyber insurance, but the premiums were too high, and we were not sure what was covered."

K. Cybersecurity Culture is Improving (n=2)

A few respondents noted that awareness of cybersecurity is gradually improving within the SME sector. They attributed this shift to increased media coverage of cyber threats and occasional security training initiatives. One participant remarked, "We have started paying more attention to security after hearing about businesses like ours being hacked."

IV. DISCUSSION

This study makes a significant contribution to understanding the cybersecurity challenges faced by Small and Medium-sized Enterprises (SMEs) in Nigeria-an increasingly critical area given the growing reliance on digital technologies for business operations [5]-[7]. It is among the first to analyse the prevalence and severity of unpatched vulnerabilities in Nigerian SMEs, with a specific focus on the human and technical constraints that hinder the implementation of effective cybersecurity measures [1], [8]. By capturing real-world cybersecurity challenges through direct responses from SME owners and IT managers, the study offers valuable insights into the practical difficulties these businesses encounter [2], [3].

This research addresses a crucial gap by focusing on SMEs, which are often overlooked in cybersecurity studies that typically concentrate on larger enterprises [5], [7], [9]. The inclusion of a sample of 100 SMEs across various industries enhances the study's generalizability by providing a diverse representation of sectors, thereby offering a more comprehensive view of cybersecurity practices and challenges [10]-[12]. The use of an anonymous web-based survey facilitated the collection of candid responses, reducing response bias and improving data reliability [11], [12]. However, a limitation of this approach is that self-reported data may introduce biases, as participants might underreport or exaggerate cybersecurity incidents due to personal or organizational concerns [12], [13]. Despite this limitation, self-reported surveys remain a widely accepted method in cybersecurity research, particularly for assessing organizational security, as they provide insights into internal practices and perceptions that are otherwise difficult to measure [11], [12].

The study identified several recurring cybersecurity challenges among SMEs, including unpatched vulnerabilities, social engineering threats, financial constraints, and overall security gaps, all of which contribute to heightened cyber risk exposure. Unpatched software and social engineering attacks are particularly concerning, as they exploit common vulnerabilities and human error, making SMEs attractive targets for cybercriminals. Unpatched systems are susceptible to known exploits, while social engineering attacks manipulate human behaviour to gain unauthorized access to sensitive information-tactics often observed in phishing and pretexting attacks [14]-[16], [31]. Similar studies in other developing economies show that SMEs struggle with cybersecurity due to limited technical expertise and financial resources, which hinder their ability to implement robust security measures and stay ahead of evolving threats [15], [17], [18], [32]. SME owners often perceive cybersecurity costs as prohibitive, resulting in delays in security updates and increased exposure to threats. Financial constraints make it difficult to prioritize cybersecurity investments [15], [17]. Additionally, some respondents noted a lack of formal cybersecurity training for employees, underscoring the need for targeted awareness programs to mitigate human vulnerabilities and strengthen the overall security posture [15], [16], [19], [33], [34].

Opinions on cybersecurity investment remain divided. While some SMEs view it as a strategic necessity comparable to other critical business investments, others regard it as an optional expense-reflecting broader debates about investing in emerging technologies [20]-[22]. Although certain SMEs recognize the importance of cybersecurity in protecting against potential threats, many perceive it as a financial burden due to limited resources and competing business priorities [23]-[25]. Notably, only 29% of surveyed SMEs reported having a dedicated cybersecurity budget, highlighting a substantial gap between financial constraints and the need for robust security measures [26], [27].

Therefore, it is essential to develop sector-specific, cost-effective cybersecurity training and affordable security solutions to improve the resilience of SMEs against cyber threats [23], [28]-[30].

V. CONCLUSION

This study highlights the persistent cybersecurity challenges confronting SMEs in Nigeria, particularly the impact of unpatched vulnerabilities, social engineering threats, technical and IT infrastructure constraints on their overall security posture. The findings emphasize the urgent need for targeted interventions that address both technical weaknesses and human factors contributing to cyber risks.

A key insight from this research is the limited prioritization of cybersecurity investments, with only 29% of SMEs allocating a dedicated budget for security measures. These limitations, coupled with low cybersecurity awareness and ineffective security practices, increases exposure to cyber threats such as social engineering attacks, impersonation scams, and unpatched software vulnerabilities. Addressing these risks requires cost-effective, scalable security solutions tailored to SMEs, along with practical policies that enhance compliance without adding excessive financial burdens.

Moving forward, collaborative efforts between policymakers, industry stakeholders, and SMEs are essential to enhancing cybersecurity resilience. Further recommendations are: (1) compulsory, subsidized cybersecurity training for SMEs, enforced by government and NGOs; (2) development of lightweight security tools for SMEs with limited infrastructure; and (3) mandatory integration of cybersecurity awareness into all entrepreneurship programs with non-compliant businesses facing penalties, including suspension of registration or exclusion from public contracts. Implementing sector-specific training, affordable security frameworks, and regulatory incentives can help bridge the gap between financial constraints and the pressing need for robust security measures. Proactively addressing these challenges will strengthen SMEs' defenses against cyber threats and support sustainable digital business operations in an increasingly interconnected economy without business disruption and loss of trust in businesses.

ACKNOWLEDGEMENT

The authors, Aminu Muhammad Auwal and James Olaoluwa Abiodun gratefully acknowledge the support of their respective institutions, the University of Jos and the Federal Polytechnic Bida, Nigeria for providing an enabling environment for this research. We also appreciate the SMEs who shared their experiences, which enriched this study.

Declaration of Conflicting Interests
The authors declare no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding
The authors received no financial support for the research, authorship, and/or publication of this article.

Use of Artificial Intelligence (AI)-Assisted Technology for Manuscript Preparation
The authors confirm that no AI-assisted technologies were used in the preparation or writing of the manuscript, and no images were altered using AI.

REFERENCES

[1] L. Bamidele, L. Benjamin, A. Adegbola, P. Amajuoyi, M. Adegbola, and K. Adeusi, "Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies," *Glob. J. Eng. Technol. Adv.*, 2024. [Online]. Available: https://doi.org/10.30574/gjeta.2024.19.2.0084.

[2] E. Onatuyeh *et al*., "Cybersecurity and business survival in Nigeria: Building customer's trust," *Afr. J. Appl. Res.*, vol. 11, no. 1, 2025. [Online]. Available: https://doi.org/10.26437/ajar.v11i1.882.

[3] S. Ewuga, Z. Egieya, A. Omotosho, and A. Adegbite, "Comparative review of technology integration in SMEs: A tale of two economies - The United States and Nigeria," *Eng. Sci. Technol. J.*, vol. 4, no. 6, 2023. [Online]. Available: https://doi.org/10.51594/estj.v4i6.680.

[4] F. Ikuero, "Preliminary review of cybersecurity coordination in Nigeria," *Niger. J. Technol.*, vol. 41, no. 3, 2022. [Online]. Available: https://doi.org/10.4314/njt.v41i3.11.

[5] C. Jerome, J. Ezinne, and K. Abia, "Cybersecurity challenges in Nigeria: The way forward," *Oforji*, 2017.

[6] E. Onatuyeh *et al*., "Cybersecurity and business survival in Nigeria: Building customer's trust," *Afr. J. Appl. Res.*, vol. 11, no. 1, 2025. [Online]. Available: https://doi.org/10.26437/ajar.v11i1.882.

[7] H. Ukwuoma, I. Williams, and I. Choji, "Digital economy and cybersecurity in Nigeria: Policy implications for development," *Int. J. Innov. Digit. Econ.*, vol. 13, pp. 1–11, 2022. [Online]. Available: https://doi.org/10.4018/ijide.292489.

[8] Y. Ibrahim *et al*., "Cybersecurity and cybercrimes in Nigeria: An overview of challenges and prospects," in *Proc. 2024 Int. Conf. Sci., Eng. Bus. Driving Sustainable Development Goals (SEB4SDG)*, 2024, pp. 1–7. [Online]. Available: https://doi.org/10.1109/SEB4SDG60871.2024.10630301.

[9] A. Iorliam, "Cybersecurity and mobile device forensic," in *Cybersecurity in Nigeria*, Springer, 2019. [Online]. Available: https://doi.org/10.1007/978-3-030-15210-9_4.

[10] J. De Arroyabe, M. Arroyabe, I. Fernandez, and C. Arranz, "Cybersecurity resilience in SMEs: A machine learning approach," *J. Comput. Inf. Syst.*, 2023. [Online]. Available: https://doi.org/10.1080/08874417.2023.2248925.

[11] L. Wong, V. Lee, G. Tan, K. Ooi, and A. Sohal, "The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities," *Int. J. Inf. Manag.*, vol. 66, p. 102520, 2022. [Online]. Available: https://doi.org/10.1016/j.ijinfomgt.2022.102520.

[12] M. Neri, F. Niccolini, and L. Martino, "Organizational cybersecurity readiness in the ICT sector: A quanti-qualitative assessment," *Inf. Comput. Secur.*, vol. 32, pp. 38–52, 2023. [Online]. Available: https://doi.org/10.1108/ics-05-2023-0084.

[13] Q. Aigbefo, Y. Blount, and M. Marrone, "The influence of hardiness and habit on security behaviour intention," *Behav. Inf. Technol.*, vol. 41, pp. 1151–1170, 2020. [Online]. Available: https://doi.org/10.1080/0144929X.2020.1856928.

[14] Z. Wang, H. Zhu, and L. Sun, "Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods," *IEEE Access*, vol. 9, pp. 11895–11910, 2021. [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3051633.

[15] J. Olaniyan and A. Ogunola, "Protecting small businesses from social engineering attacks in the digital era," *World J. Adv. Res. Rev.*, 2024. [Online]. Available: https://doi.org/10.30574/wjarr.2024.24.3.3745.

[16] W. Syafitri, Z. Shukur, U. Mokhtar, R. Sulaiman, and M. Ibrahim, "Social engineering attacks prevention: A systematic literature review," *IEEE Access*, 2022, pp. 1–1. [Online]. Available: https://doi.org/10.1109/ACCESS.2022.3162594.

[17] G. White, R. Allen, A. Samuel, A. Abdullah, and R. Thomas, "Antecedents of cybersecurity implementation: A study of the cyber-preparedness of U.K. social enterprises," *IEEE Trans. Eng. Manag.*, pp. 1–12, 2020. [Online]. Available: https://doi.org/10.1109/TEM.2020.2994981.

[18] N. Wulandari, M. Adnan, and C. Wicaksono, "Are you a soft target for cyber-attack? Drivers of susceptibility to social engineering-based cyber-attack (SECA): A case study of mobile messaging application," *Hum. Behav. Emerg. Technol.*, 2022. [Online]. Available: https://doi.org/10.1155/2022/5738969.

[19] N. Beu *et al*., "Falling for phishing attempts: An investigation of individual differences that are associated with behavior in a naturalistic phishing simulation," *Comput. Secur.*, vol. 131, p. 103313, 2023. [Online]. Available: https://doi.org/10.1016/j.cose.2023.103313.

[20] M. Chronopoulos, E. Panaousis, and J. Grossklags, "An options approach to cybersecurity investment," *IEEE Access*, vol. 6, pp. 12175–12186, 2018. [Online]. Available: https://doi.org/10.1109/ACCESS.2017.2773366.

[21] A. Fedele and C. Roner, "Dangerous games: A literature review on cybersecurity investments," *J. Econ. Surv.*, 2021. [Online]. Available: https://doi.org/10.1111/joes.12456.

[22] J. Simon and A. Omar, "Cybersecurity investments in the supply chain: Coordination and a strategic attacker," *Eur. J. Oper. Res.*, vol. 282, pp. 161–171, 2020. [Online]. Available: https://doi.org/10.1016/j.ejor.2019.09.017.

[23] S. Armenia, M. Angelini, F. Nonino, G. Palombi, and M. Schlitzer, "A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs," *Decis. Support Syst.*, vol. 147, p. 113580, 2021. [Online]. Available: https://doi.org/10.1016/J.DSS.2021.113580.

[24] M. Arroyabe, C. Arranz, I. De Arroyabe, and J. De Arroyabe, "Exploring the economic role of cybersecurity in SMEs: A case study of the UK," *Technol. Soc.*, 2024. [Online]. Available: https://doi.org/10.1016/j.techsoc.2024.102670.

[25] A. Alahmari and R. Duncan, "Investigating potential barriers to cybersecurity risk management investment in SMEs," in *Proc. 2021 13th Int. Conf. Electron., Comput. Artif. Intell. (ECAI)*, 2021, pp. 1–6. [Online]. Available: https://doi.org/10.1109/ECAI52376.2021.9515166.

[26] I. De Arroyabe, C. Arranz, M. Arroyabe, and J. De Arroyabe, "Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019," *Comput. Secur.*, vol. 124, p. 102954, 2022. [Online]. Available: https://doi.org/10.1016/j.cose.2022.102954.

[27] S. Kabanda, M. Tanner, and C. Kent, "Exploring SME cybersecurity practices in developing countries," *J. Organ. Comput. Electron. Commer.*, vol. 28, pp. 269–282, 2018. [Online]. Available: https://doi.org/10.1080/10919392.2018.1484598.

[28] T. Boonen, Y. Feng, and Z. Tong, "Cybersecurity investments and cyber insurance purchases in a non-cooperative game," *ASTIN Bull.*, 2025. [Online]. Available: https://doi.org/10.1017/asb.2024.40.

[29] M. Marican, S. Razak, A. Selamat, and S. Othman, "Cybersecurity maturity assessment framework for technology startups: A systematic literature review," *IEEE Access*, vol. 11, pp. 5442–5452, 2023. [Online]. Available: https://doi.org/10.1109/ACCESS.2022.3229766.

[30] O. O. Blaise, I. Aaron, U. Alfred, and A. Amusa, "Evaluating the ethical frameworks of information security professionals: A comparative analysis," *Asian J. Comput. Sci. Technol.*, vol. 13, no. 2, pp. 61–66, Nov. 2024. [Online]. Available: https://doi.org/10.70112/ajcst-2024.13.2.4289.

[31] M. S. Islam, M. Sajjad, M. M. Hasan, and M. S. I. Mazumder, "Phishing attack detecting system using DNS and IP filtering," *Asian J. Comput. Sci. Technol.*, vol. 12, no. 1, pp. 16–20, 2023. [Online]. Available: https://doi.org/10.51983/ajcst-2023.12.1.3552.

[32] S. Ravichandran and K. L. N. Rao, "Design and development of an advancing web information stockpiling for engraved ontology in user contours," *Asian J. Comput. Sci. Technol.*, vol. 11, no. 2, pp. 11–15, 2022. [Online]. Available: https://doi.org/10.51983/ajcst-2022.11.2.3379.

[33] K. A. Y. Yaseen, "Importance of cybersecurity in the higher education sector," *Asian J. Comput. Sci. Technol.*, vol. 11, no. 2, pp. 20–24, 2022. [Online]. Available: https://doi.org/10.51983/ajcst-2022.11.2.3448.

[34] A. M. Auwal and S. Lazarus, "Sociological and criminological research of victimization issues: Preliminary stage and new sphere of cybercrime categorization," *J. Digit. Technol. Law*, vol. 2, no. 4, pp. 915–942, 2024. [Online]. Available: https://doi.org/10.21202/jdtl.2024.44.