2025; 1-2 | pp.142-148

International Journal of Advances in Engineering and Computer Science ISSN: 3121-6382

Volume 1, Issue 2, October-December, 2025
(An Academians Publishers of Research & Academic Resources)

Review Article

Received: 18-10-2025 Accepted: 25-11-2025 Published: 05-12-2025

Awareness of Information Security Best Practice Among Small and Medium Enterprises (SMEs)

Zaharaddeen Abdullahi[1], Falalu Ahmad Khalipha[2], Shamsuddeen Mohammed Lawal[3]
[123]*Computer Science Department*
Katsina State Institute of Technology & Management

Abstract: Cybersecurity awareness remain the most critical for defending small and medium enterprises (SMEs) against the growing threats of cyber-attacks in current digital era. In spite of their important contribution to national economy, SMEs in Nigeria, continue to be the centre of cyber-attacks due to inadequate awareness, inadequate resources, and poor knowledge of cybersecurity measures required. This study examines the level of SMEs information security awareness in Nigeria, exploring the factors influencing their cybersecurity knowledge and practices, as well as evaluates the effect of these awareness on their daily operational resilience. This paper adopted a mixed-methods research techniques, data were collected from various SMEs sectors using structured questionnaires and interviews. The findings reported low cybersecurity awareness, financial constraints, lack of training, and perceived irrelevance of cybersecurity as major barriers as challenges. Therefore, study recommends critical need for specified interventions such as affordable training programs, government-led initiatives, and enhanced community awareness campaigns. These recommendations intend to empower SMEs to build robust cybersecurity culture to safeguard their daily operations and contribute to sustainable economic growth.

Keywords: *Cybersecurity, SMEs, MSME, Information Security, Computer, Internet*

1. Introduction

Small and medium enterprises (SMEs) is critical to nation economic growt' contributing significantly to GDP ana employment in Nigeria. NBS/SMEDAN 2021 survey report narrated that MSMEs contributed up to 46.32% to GDP, accounted for 6.21% of exports, 96.9% of businesses and 87.9% of employment (PwC, 2024). Despite this contribution, the transformation of businesses to digital state exposes the SMEs to rising cyberattacks. The growing interest of cybercriminals towards SMEs reveals their vulnerability, situating them in wide range of risks such as phishing scams, ransomware attacks, and data breaches. Nigerian SMEs are underprepared for these cybersecurity challenges due to insufficient awareness, limited resources, and weak enforcement of cybersecurity policies.

Globally, SMEs are excessively affected by cyber threats. A study conducted by Ponemon Institute (2019) indications that SMEs account for 43% of the overall cyberattacks, 60% of the affected SMEs often goes out of business within six months of the data breach. Adepetun (2018) studies conducted in Nigeria reveal that 89% of cyberattacks in 2022 targeted SMEs, one of the reasons behind it is mostly due to their lack of basic defensive measures such as adequate awareness, firewalls, intrusion detection systems, and staff training. Moreover, SMEs in state like Katsina, face added challenges such as limited

Corresponding Author: Zaharaddeen Abdullahi

access to affordable cybersecurity tools and lack of institutional support because most of IT resources and services are situated in either Lagos or Abuja (Kabanda Tanner & Kent, 2018). Bada and Nurse (2019) debates that the inadequate tailored awareness among SMEs increases their vulnerability, suggesting that context-based interventions remain necessary to drive meaningful transformation.

Huge number if not all Nigerian enterprises lack adequate awareness and preparedness for cyber threats, leaving them exposed to breaches, fraud, and other cyberattacks. Among the factors that contributed to their current state of cyber insecurity is inadequate awareness. Thus, this study explores the awareness levels and challenges faced by SMEs in Katsina in relation to network and information security, aiming to propose actionable recommendations for improvement.

The rapid development and digitization of businesses across the globe, Africa and Nigeria specifically has introduced better opportunities and wide range of risks for SMEs in cyber world. Despite the critical role they are playing in economic growth, SMEs in Nigeria often operate with limited resources, making them prime targets for cybercriminals (Bada & Nurse, 2019). In Katsina, major of SMEs rely on digital platforms for advertisement, financial transactions, and customer relations etc. However, inadequate awareness of information security measures leads to vulnerabilities such as fraud, phishing scams, and/or even ransomware attacks (Adepetun, 2022). This situation worsens by inadequate cybersecurity initiatives targeting SMEs from both governmental and non-governmental organizations leaving them without adequate tools or training to protect themselves. Thus, this study sought to investigates the level of awareness and challenges of SMEs in relations to information security in Katsina. The questions this study seek to evaluate is the awareness state of contemporary entrepreneurs of cybersecurity best practice to set a baseline data and ascertain gaps and challenges in implementing these best practices and recommends strategies for improving cybersecurity best practices among SMEs.

1. Literature Review

SMEs in Nigeria are increasingly facing outmost cyber threats despite their significant contribution to her economy. This challenge has been creating loopholes in their capacity to serve the country better. SMEs cyber related risk is making millions if not billions of Naira go to waste every year. This may be due their inadequate training or awareness of cybersecurity measures necessary to depend themselves. Ogbeide, Omorogiuwa and Salami (2023) proposed a robust yet cost effective cybersecurity framework that can be adopted by SMEs to help them develop resilience and stay informed in the cyber world. One of the key aspect of their framework is employee awareness and training.

Almost all internationally recognize cybersecurity frameworks include awareness and training of employee on the current practices and measures needed to mitigate threats. Ogbeide et al. (2023) reviewed six international frameworks and lamented that every one of the framework remain incomplete if employee awareness and training is eliminated. Okoye (2017) in her study on strategies to minimize threats on business performance specifies that organizational information security education and training was found to be significant part of performance indicators of SMEs in the current century. In their research in UK Bada and Nurse (2019) insisted that though theoretical aspect of awareness and training is widely delivered, they found it to be less effective in real world scenarios. They suggest that practical engagements should be included during training to enable employee assimilate the strategies better. Erdogan, Halvorsrud, Boletsis, Tverdal and Pickering (2023) lamented that though SMEs in UK

apply some basic cybersecurity measures to avert cyber threats, there seems to be inadequate training and awareness as well as processes and tools necessary to improve their information security posture. Amrin (2014) in her study on the impact of cybersecurity on SMEs in Europe, insists that lack of employee training and awareness especially in Bring Your Own Devices (BYOD) and cloud related work culture shouldered huge risk to the SMEs. There is lack or inadequate news and trends of cyber threats as well as mitigation measures among SMEs in Nigeria and the world at large.

Fagbule (2021) lamented that SMEs fall victim of cyber related incidences due to their lack or limited budget in employee training and awareness. Employee often follow organizational culture. When an organizational lack information security culture or framework, its employee often neglect or shortfall cybersecurity measures to mitigate known threats. She concluded that IT technical staff neglects important cybersecurity awareness and training points due to their lack or limited understanding of their organizational culture and attitude. Erdogan et al. (2023) study provides better understanding of SME context in terms of cybersecurity awareness and cybersecurity practices, and may be used as a foundation to further develop appropriate tools and processes to strengthen the cybersecurity of SMEs that accorded their culture and attitude. Carlos, Ingolf and Shane (2023) reports that there is limited research on SMEs roles threats and needs related to cybersecurity. They further insisted that lack of awareness of cybersecurity risks, limited literacy and financial constraints. The study concluded that there exists significant relationship among these themes, suggesting that limited literacy is the root cause of awareness and resource constraint issues.

3. Methodology

The study adopted a mixed-methods approach, combining both quantitative surveys and literature review to gather comprehensive insights. Scoping literature on cybersecurity awareness and education in Nigeria was conducted in the first phase of the study. This theoretical review was followed by a fieldwork on current status of SMEs cybersecurity awareness, their contemporary challenges and suggested ways to mitigate it. From these analyses, we compared their level in 3 aspects above and suggest key lessons/recommendations to create high level cybersecurity awareness and training among SMEs.

25 randomly selected SMEs across various sectors in Katsina, including retail, commercial, and service industries were sampled. A stratified random sampling technique was used because it gives each member of strata equal chance to be selected. Structured questionnaires for quantitative data and focus group discussion for qualitative insights. Quantitative data collected was analyzed using statistical software to identify correlations to uncover recurring patterns and challenges.

4. Results and Discussions

Table 4.1: The contemporary level of cybersecurity awareness among SMEs in Katsina

Category	Frequency	Percentages
Network security (such as strong password, firewall, up-to-date antivirus, device security patches)	7	25%
Physical security (such as barriers, cctv, watchmen etc.)	23	82.2%
Strong password and its changes frequently	6	21.4%
Antivirus protection and regular software updates	11	39.2%
Information security education, training and awareness	7	25%
Data backup and recovery	17	60.7%
Network security monitoring and audit	0	0%

Intrusion detection	0	0%
People Management (e.g. Ex-employee decommissioning)	3	10.7%
Asset management (e.g. Faulty devices decommissioning)	0	0%
Overall (Average)	**28**	**26.42%**

The study findings reveal that only 26.42% of SMEs in Katsina are sentient of the existing measures of network and information security related to their businesses. Physical security measures such as barriers, CCTV, and watchmen were testified as the most widely adopted security practices. It is the top priority is consistent with findings where physical threats are more widespread than cyber risks. This finding is supported by Adetunji, Olalekan, & Idowu, (2022) who lamented that SMEs in such kind of regions heavily relying on tangible security measures. It was also reveal that a significant number (60.7%) of SMEs are mindful of the significance of data backup and recovery, highlighting a basic understanding of data protection practices. However, these adoption does not extend to more sophisticated or hands-on digital security measures like intrusion detection. The adoption rate of data backup remains encouraging because it is slightly higher than reported averages in similar regions (50%-55%, as per UNCTAD, 2020). However, the efficacy of these backups depends on regular testing.

No SMEs testified using network security monitoring, audits, or intrusion detection systems, which shows either lack of either means or awareness of these critical measures. This remains one of the gap leaving businesses vulnerable to cyber threats especially in digital era of today, as these are some of the foundational does for robust cybersecurity frameworks. In the other hand, antivirus protection and regular system updates are admitted, although the percentage stands relatively low compared to global standards. This further underscores inadequate understanding or practices of basic cyber hygiene. Studies submit that SMEs worldwide often prioritize cost-effective and basic security measures, such as antivirus and firewalls software, while cutting-edge techniques like intrusion detection systems are less commonly used due to resource constraints (Ahmad, Burney & Malik, 2021). This also aligns with the findings in Katsina, where physical security dominates, while cyber and network security practices are vague.

Only a one fourth of SMEs reported information security education and training, highlighting an awareness gap that hinders the implementation of comprehensive security practices. Research by Von Solms & Van Niekerk (2013) stresses that security awareness training is the foundation of organizational cybersecurity. The low percentage (25%) of training adoption rate in Katsina echoes the global challenge of prioritizing security training in SME levels. Practices such as decommissioning faulty devices or managing access for ex-employees are found unaddressed, further presenting significant risks in maintaining security posture of an organization. The absence of network security monitoring and audits in Katsina SMEs bluntly contrasts with global best practices, where such measures are ranked critical as highlighted by Srinivas et al. (2020) noting that even basic monitoring significantly reduces cyber risks.

Table 4.2: Gaps and barrier for implementation of security measures

Challenges	Frequency	Percentages
Inadequate information security education, training and awareness	19	67.9
Lack of network and information security tools	13	46.4
Perceived irrelevance	16	57.2%
Lack of regular updates and software security patches.	9	32.2%
Limited resources	14	50%
Weak cybersecurity policy enforcement	19	67.9%
Inadequate implementation of cybersecurity policies	21	75%
Overall (Average)	**28**	**56.67%**

The study recognizes several challenges that SMEs in Katsina face while implementing robust information security measures. These challenges combine a combination of resource constraints, knowledge gaps, and policy enforcement issues.

It was also reported that the most significant barriers hindering effective implementation of information security measures is reflecting a lack of foundational knowledge and skills among SME employees and management. Without appropriate training, SMEs will continue to struggle distinguishing threats, mitigate risks, and adopt effective security measures. As testified by Von Solms & Van Niekerk (2013) and Ahmad et al. (2021) who highlighted that inadequate training is a universal challenge, especially for SMEs. Thus the 67.9% lack of inadequate awareness found is in line with global averages, where awareness campaigns mostly target larger organizations situated in larger cities across the globe. Moreover, absence of reliable security enforcement mechanisms means even when policies exist, they are often not abided by. This leads to wide range of vulnerabilities, from human fault, carelessness, or deliberate bypass of security protocols. This lack of policy enforcement and implementation is supported by findings in developing regions where regulatory frameworks and policies are weak or poorly enforced (UNCTAD, 2020). Globally, SMEs often report challenges in translating cybersecurity policies into actionable steps due to limited expertise (Pwc, 2024).

The challenges further indicate that even with an avocations of the need for policies, practical implementation lags significantly. This gap further worsens the disconnection between knowledge and action, possibly due to resource, awareness or expertise shortages. Financial limitations remain a persistent reason behind inadequate cybersecurity measure adoption. Srinivas et al. (2020) narrated that about 55% of SMEs globally faces budget constraints as the primary obstacle, which align with the finding of 50% in this data. Several SMEs consider cybersecurity as non-factor thinking that they are not targets for cyberattacks. This mindset and attitude places them exposed to risks, as SMEs are increasingly targeted by attackers due to weaker defenses. This finding is in line with Kshetri, (2019) who reported that, cybersecurity is considered not a priority for small businesses has been documented widely which stems from a lack of awareness of evolving cyber threats targeting SMEs.

5. Conclusion

Cybersecurity awareness remain a cornerstone of information security resilience for SMEs. The findings emphasize the significant gaps in the information security practices of SMEs in Katsina, with an inconsistent focus on physical security over digital ones as well as the high percentage of irrelevance as shown. This trend, while consistent with developing regions, highlights the urgent need for awareness, training, and resource allocation to address cybersecurity vulnerabilities especially among developing businesses. By

comparing these results with global benchmarks, it's clear that targeted interventions can significantly enhance the overall security posture of SMEs in Katsina. The findings highlight the urgent need for targeted interventions to enhance their preparedness. Recommendations include:

1. There is need for government-led initiatives to establish subsidized cybersecurity training programs for SMEs.
2. There is also need for partnerships and collaboration with tech companies to provide affordable security tools tailored for small businesses.
3. There should be a routine awareness campaigns through door to door, community outreach programmes, public seminars and online workshops to educate SME owners and employees about emerging threats and best practices.
4. There is urgent need for up to date and regular assessments to encourage SMEs to conduct routine internal audits of their cybersecurity posture to identify and address vulnerabilities to ensure adherence to cybersecurity best practice.

References

Adepetun, A. (2022). Cyberattack on Nigerian SMEs up by 89 per cent in 2022. *The Guardian Nigeria News*. Retrieved from https://guardian.ng/business-services/cyber-attack-on-nigerian-smes-up-by-89-per-cent-in-2022.

Adetunji, O. O., Olalekan, A., & Idowu, F. (2022). Enhancing SMEs' cybersecurity resilience in Nigeria: Challenges and solutions. *Journal of Cybersecurity and Digital Forensics*, *12*(2), 101–112.

Ahmad, F., Burney, A., & Malik, A. (2021). Security aspects of virtualization and its impact on business information security. *IEEE International Conference on Information Science and Communication Technology (ICISCT)*, 1-5. https://doi.org/10.1109/ICISCT49550.2020.9080029

Amrin, N. (2014). The Impact of Cyber Security on SMEs. Thesis of University of Twente.

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for SMEs. *Information and Computer Security, 27*(3), 406–417. https://doi.org/10.1108/ICS-07-2018-0080

Carlos R. J., Ingolf, B., & Shane, J. (2023). Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity. 1(1), 1 – 32.

Erdogan, G., Halvorsrud, R., Boletsis, C., Tverdal, S. & Pickering, J. (2023). *Cybersecurity Awareness and Capacities of SMEs.* In Proceedings of the 9th International Conference on Information Systems Security and Privacy (ICISSP 2023), 296-304.

Fagbule, O. (2021). Cyber Security Training in Small to Medium-sized Enterprises (SMEs): Exploring Organisation Culture and Employee Training Needs. Thesis of Bournemouth University.

Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce, 28*(3), 269–282. https://doi.org/10.1080/10919392.2018.1484598

Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management, 22*(2), 77–81. https://doi.org/10.1080/1097198X.2019.1603527

Ogbeide, V.O., Omorogiuwa, O & Salami, E.E. (2023). A cybersecurity

framework to strengthen small and medium scale enterprises (SMEs) in Nigeria. *International Journal of Science Academic Research,* 4(9), 6301-6310.

Okoye, F.B. (2017). Strategies to Minimize the Effects of Information Security Threats on Business Performance. Dissertation of Walden University, UK.

Ponemon Institute. (2019). *Global State of Cybersecurity in Small and Medium-Sized Businesses*. Retrieved from https://www.cisco.com/c/dam/en/us/products/collateral/security/ponemon-report-smb.pdf.

Pwc (2024). PcW MSME Survey. Retrieved from https://www.pwc.com/ng/en/assets/pdf/2024-pwc-msme-survey-report.pdf

Small and Medium Enterprises Development Agency of Nigeria (SMEDAN). (2021). *National Policy on Micro, Small and Medium Enterprises*. Abuja: SMEDAN.

Srinivas, J., Das, A. K., & Kumar, N. (2020). Government regulations in cybersecurity: Framework, standards, and recommendations. *Future Generation Computer Systems, 107*, 171–185. https://doi.org/10.1016/j.future.2019.12.041

United Nations Conference on Trade and Development (UNCTAD). (2020). *Cybersecurity challenges facing SMEs in developing economies*. Retrieved from https://unctad.org.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cybersecurity. *Computers & Security, 38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004