International Journal of Computer Science and Mathematical Theory (IJCSMT) E-ISSN 2545-5699
P-ISSN 2695-1924 Vol 11. No. 5 2025 www.iiardjournals.org online version

Bridging the Cybersecurity Gap in Nigerian SMEs: An Empirical Study of Awareness and Practice

Adamu Abdulmalik[1]
Computer Science Department Federal College of Education,
Yola, Adamawa State, Nigeria
adamalik@fceyola.edu.ng
Phone: 08038040367

Mohammed, Usman[2]
Computer Science Department Federal Polytechnic,
Bali Taraba State, Nigeria
shaggyrancy@gmail.com
Phone: 08143484439

Bello Fatima Hamid[3]
Computer Science Department Federal College of Education,
Yola, Adamawa State, Nigeria
fatimabello30@gmail.com
Phone: 07064448424
DOI: 10.56201/ijcsmt.vol.11.no5.2025.pg93.101

Abstract
The increasing digitization of business operations in Nigeria has heightened the urgency for effective cybersecurity awareness and implementation. This study investigates the current state of cybersecurity awareness, the adoption of protective measures, and the challenges businesses face in implementing cybersecurity protocols. Using a survey of 162 Nigerian business respondents, the research reveals that while a moderate level of awareness exists, the adoption of advanced security practices remains limited. Basic tools such as antivirus software are widely used, yet more strategic defenses like multi-factor authentication and employee training are significantly underutilized. Key challenges identified include lack of technical expertise, financial constraints, and minimal organizational support. The findings underscore the need for targeted capacity building, government incentives, and a cultural shift toward proactive cybersecurity management. Addressing these issues holistically will be critical in fortifying Nigeria's business ecosystem against escalating cyber threats.

Keywords*: Cybersecurity awareness, Nigerian businesses, cybersecurity adoption, technical expertise, cyber threat mitigation.*

1. Introduction

In today's digital era, cybersecurity has emerged as a critical concern for businesses worldwide. In Nigeria, the rapid digital transformation across sectors such as finance, healthcare, and governance

has heightened the importance of robust cybersecurity measures. Despite this, many Nigerian businesses, particularly small and medium-sized enterprises (SMEs), exhibit low levels of cybersecurity awareness and adoption, rendering them vulnerable to cyber threats.

The Nigerian Communications Commission (NCC) reported a 30% increase in cyberattacks in 2022, underscoring the escalating threat landscape (Ejeofobiri, 2023). This surge in cyber threats is attributed to factors such as limited awareness, inadequate infrastructure, and a shortage of skilled cybersecurity professionals. Many businesses underestimate the risks associated with cyberattacks, leading to lax security practices like using weak passwords and neglecting software updates (Independent Newspaper Nigeria, 2023).

The skills gap in cybersecurity is another pressing issue. The demand for qualified cybersecurity professionals outpaces supply, making it challenging for businesses to recruit competent staff (Businessday NG, 2023). This shortage is exacerbated by limited resources for training and certifying individuals in cybersecurity.

Inadequate infrastructure further compounds the problem. Many organizations rely on outdated systems and software lacking modern security features, making them susceptible to cyberattacks (Independent Newspaper Nigeria, 2023). The lack of investment in secure software and hardware, such as firewalls and encryption devices, leaves networks exposed to potential breaches.

To address these challenges, leveraging emerging technologies like Artificial Intelligence (AI) can enhance cybersecurity awareness and education. AI-driven adaptive learning systems can tailor training content based on individual user behaviors, providing personalized and context-aware awareness training (Olatunji, 2023). Additionally, AI can analyze vast amounts of threat intelligence data in real-time, identifying emerging threats and providing timely updates to awareness programs.

Public-private partnerships are crucial in fostering a cybersecurity-conscious society. Collaborations between government agencies, educational institutions, and private sector entities can facilitate the development of comprehensive training programs and awareness campaigns (ISSAN, 2024). These initiatives should aim to educate individuals and organizations about cybersecurity threats and safe online practices.

Furthermore, legal frameworks like the Nigeria Data Protection Act 2023 impose obligations on businesses to secure their IT infrastructure and protect customer data. Non-compliance can result in significant penalties, emphasizing the need for businesses to prioritize cybersecurity measures (The Firma Law Practice, 2023).

Enhancing public awareness and adoption of cybersecurity practices among Nigerian businesses is imperative. Addressing the challenges of limited awareness, skills gap, and inadequate infrastructure requires a multifaceted approach involving technological innovation, education, and regulatory compliance. By fostering a culture of cybersecurity consciousness, Nigeria can safeguard its digital economy against the growing threat of cyberattacks.

Statement of the Problem

Despite the increasing prevalence of cyber threats in Nigeria, many businesses—especially small and medium-sized enterprises (SMEs)—remain inadequately informed and ill-prepared to combat cybersecurity risks. Public awareness of cybersecurity practices is still relatively low, and the adoption of preventive measures is inconsistent across different business sectors. Reports from national cybersecurity stakeholders indicate a sharp rise in cyberattacks, ranging from phishing

and ransomware to data breaches and financial fraud (Independent Newspaper Nigeria, 2023). The limited integration of cybersecurity protocols, lack of skilled personnel, and poor understanding of regulatory requirements leave Nigerian businesses vulnerable to operational disruption, reputational damage, and financial loss. This growing concern underscores the urgent need for a deeper understanding of current awareness levels and the barriers preventing effective adoption of cybersecurity practices among Nigerian businesses.

Aim

This study aimed to assess the level of public awareness and the extent of adoption of cybersecurity practices among Nigerian businesses, with a view to identifying key challenges and proposing strategies to improve cybersecurity preparedness.

Objectives

1. To evaluate the current level of awareness of cybersecurity threats and practices among Nigerian business owners and employees.
2. To assess the extent to which Nigerian businesses have adopted cybersecurity policies, tools, and protocols.
3. To identify the key barriers—technological, educational, financial, or regulatory—hindering the effective implementation of cybersecurity measures in Nigerian enterprises.

2. Reviews

Conceptual Review

Cybersecurity refers to the practices and technologies designed to protect networks, devices, and data from unauthorized access, cyberattacks, or damage (Weber, 2010). In the context of business operations, cybersecurity extends beyond firewalls and encryption to include awareness, policy enforcement, and risk management strategies. In Nigeria, where digital adoption is increasing rapidly, businesses—particularly small and medium enterprises (SMEs)—are becoming more vulnerable to cyber risks due to low awareness and poor adoption of protective measures (BusinessDay NG, 2023).

Public awareness of cybersecurity involves the understanding of threats such as phishing, malware, ransomware, and data breaches, and how to mitigate them. Adoption, on the other hand, refers to the implementation of practices like secure passwords, data backup, employee training, and access control. According to ISSAN (2024), Nigerian organizations are beginning to realize the importance of cybersecurity, yet adoption remains uneven, especially among smaller firms and in rural regions.

Theoretical Review

This study is underpinned by the Technology Acceptance Model (TAM) and the Protection Motivation Theory (PMT).

Technology Acceptance Model (TAM) (Venkatesh, Thong, & Xu, 2016) posits that users' acceptance of technology is influenced by perceived usefulness and perceived ease of use. In a cybersecurity context, this theory helps explain how Nigerian businesses evaluate the benefits and challenges of adopting cybersecurity tools and practices.

Protection Motivation Theory (PMT) provides insights into how individuals are motivated to protect themselves against threats. It argues that the intention to adopt protective behavior (e.g., cybersecurity measures) is based on perceived threat severity, vulnerability, response efficacy, and self-efficacy. Nigerian businesses may adopt cybersecurity practices when they perceive high risk and believe they have the capacity and tools to mitigate those risks (Olatunji, 2023).

Both theories emphasize that awareness alone is insufficient without motivation, accessibility, and training, particularly in environments like Nigeria where digital literacy levels vary greatly (Ejeofobiri, 2023).

Empirical Review

Several empirical studies have explored cybersecurity awareness in Nigeria. For example, Tambo and Adesina (2022) examined the digital divide and found that low cybersecurity awareness and infrastructure deficiencies are key barriers to secure digital engagement in Nigerian rural areas. Soomro, Abdullah, and Faheem (2023) noted that awareness campaigns tailored to local contexts significantly improved cybersecurity behaviors among rural businesses.

ISSAN (2024) emphasized the role of national campaigns, suggesting that regular public sensitization can reduce incidents of cyber fraud. Ejeofobiri (2023) investigated how artificial intelligence can support cybersecurity education and found that interactive platforms using AI improved user understanding among Nigerian SMEs.

Moreover, The Firma Law Practice (2023) provided practical insights into how businesses can adopt cybersecurity frameworks, highlighting legal obligations and best practices. These empirical studies underscore the need for contextualized, scalable, and sustainable cybersecurity solutions for Nigerian businesses.

3. Methodology

This study employed a quantitative research design to investigate the level of public awareness and the adoption of cybersecurity practices among Nigerian businesses. The research was guided by a deductive approach, with the aim of testing existing theories and frameworks related to cybersecurity awareness and adoption. An online questionnaire was used as the primary instrument for data collection, allowing for broad distribution across various business sectors and geographical locations within Nigeria.

The questionnaire was developed using Google Forms and consisted of both closed-ended and Likert-scale questions. The instrument was structured into four sections: demographic information, awareness of cybersecurity threats, current cybersecurity practices, and perceived challenges in implementing cybersecurity measures. The design of the questionnaire was informed by previous studies on cybersecurity awareness and behavioral intention models, such as the Unified Theory of Acceptance and Use of Technology (Venkatesh et al., 2016) and localized cybersecurity assessments conducted by Nigerian researchers (Okoye & Eze, 2022).

The target population for the study included business owners, managers, IT personnel, and employees working in micro, small, medium, and large-scale enterprises across Nigeria. A non-probability purposive sampling technique was adopted to ensure that the participants were individuals with basic knowledge of their organization's digital practices. The link to the questionnaire was shared through professional networks, business forums, LinkedIn, WhatsApp groups, and email lists related to Nigerian commerce and industry.

A total of 185 responses were collected over a period of four weeks. After removing incomplete entries and responses from individuals outside the business environment, 162 valid responses were retained for analysis. Data collected were exported into Microsoft Excel and later analyzed using descriptive statistics in SPSS (Statistical Package for the Social Sciences). Frequencies, percentages, and mean scores were used to summarize the responses and identify patterns related to cybersecurity awareness, adoption levels, and implementation challenges.

Ethical considerations were duly observed in the course of this research. Participation was entirely voluntary, and respondents were informed about the purpose of the study at the beginning of the questionnaire. Confidentiality of all responses was maintained, and no personally identifiable information was collected.

The use of an online questionnaire proved effective for reaching a geographically dispersed population in a timely and cost-effective manner. The collected data offered valuable insights into the cybersecurity awareness landscape among Nigerian businesses and laid the foundation for drawing evidence-based recommendations.

4. Results and Discussion

This section presents and interprets the findings from the study on cybersecurity awareness, adoption practices, and implementation challenges among Nigerian businesses.

4.1 Awareness of Cybersecurity Threats

Table 1 presents the respondents' awareness levels regarding cybersecurity threats. The data indicate that a substantial proportion of the businesses surveyed reported being *moderately aware* (46.9%) of cybersecurity issues. A smaller segment (29.6%) identified themselves as *highly aware*, while 18.5% were *slightly aware* and only 4.9% had *no awareness*.

Table 1. Respondents' Awareness of Cybersecurity Threats

Awareness Level	Frequency	Percentage (%)
Highly Aware	48	29.6
Moderately Aware	76	46.9
Slightly Aware	30	18.5
Not Aware	8	4.9
Total	**162**	**100**

These findings suggest that while cybersecurity awareness is growing among Nigerian businesses, there remains a considerable knowledge gap. This moderate awareness level can be attributed to limited training opportunities, insufficient exposure to digital security risks, and a general lack of

cybersecurity education. Similar conclusions were drawn by Soomro et al. (2023), who emphasized that awareness in developing economies is often hindered by resource constraints and a lack of structured sensitization programs.

4.2 Adoption of Cybersecurity Practices

Table 2 highlights the extent to which specific cybersecurity practices have been adopted by the surveyed businesses. The most widely implemented measure was the use of antivirus software, with 82.1% of respondents confirming its use. Other practices, however, showed markedly lower adoption rates: regular password updates (61.7%), data backup (59.9%), multi-factor authentication (43.2%), and employee training on cybersecurity (34.0%).

Table 2. Adoption of Cybersecurity Practices by Businesses

Cybersecurity Measure	Implemented (%)	Not Implemented (%)
Use of antivirus software	82.1	17.9
Regular password updates	61.7	38.3
Multi-factor authentication	43.2	56.8
Employee cybersecurity training	34.0	66.0
Data backup practices	59.9	40.1

These statistics indicate a predominantly reactive posture toward cybersecurity, where businesses focus on basic protection while neglecting more comprehensive and preventive measures. This trend may reflect limited organizational capacity and a prioritization of immediate over strategic concerns. Okoye and Eze (2022) similarly observed that many small and medium-sized enterprises (SMEs) in Nigeria struggle with the adoption of advanced cybersecurity protocols due to financial and technical limitations.

4.3 Challenges in Implementing Cybersecurity Measures

The perceived challenges that hinder cybersecurity implementation are summarized in Table 3. A lack of technical expertise emerged as the most significant obstacle, cited by 44.4% of respondents. Financial constraints were also prominent, affecting 33.3% of businesses. Low employee awareness (14.8%) and lack of management support (7.5%) were relatively less significant but still notable.

Table 3. Perceived Challenges in Implementing Cybersecurity

Challenge	Frequency	Percentage (%)
Lack of technical expertise	72	44.4
Financial constraints	54	33.3
Low employee awareness	24	14.8
Lack of management support	12	7.5
Total	**162**	**100**

These results underscore the critical need for capacity development, particularly in technical skills and cybersecurity knowledge. Without targeted interventions—such as training programs, subsidies, and policy incentives—many Nigerian businesses will remain exposed to cyber risks. Tambo and Adesina (2022) argued for embedding cybersecurity training and support in national digital transformation strategies to mitigate these challenges.

4.4 Summary of Findings

The findings of this study provide critical insights into the state of cybersecurity preparedness among Nigerian businesses, revealing a complex interplay of awareness, adoption behaviors, and institutional challenges. The analysis of awareness levels shows that while a fair proportion of respondents (46.9%) claim moderate awareness of cybersecurity threats, only a minority (29.6%) demonstrate high awareness. This suggests a concerning gap in deep, technical understanding of cyber risks, despite increasing exposure to digital systems in business operations. Such results reflect the broader trends in many developing economies, where digital adoption outpaces cybersecurity education (Soomro et al., 2023).

The implementation of cybersecurity measures further highlights this gap. Although 82.1% of businesses have deployed antivirus software—a basic form of protection—there is a stark drop in the adoption of more sophisticated strategies. Only 43.2% of respondents use multi-factor authentication, and just 34.0% have conducted cybersecurity training for their employees. This suggests that businesses are largely reactive, prioritizing surface-level tools while neglecting more comprehensive, policy-driven measures. As noted by Okoye and Eze (2022), such trends are typical in environments where cybersecurity is perceived as a cost center rather than a strategic asset.

The reported barriers to implementation are equally telling. A lack of technical expertise (44.4%) and financial constraints (33.3%) dominate the list of challenges, indicating systemic limitations in both human and capital resources. These limitations are particularly pronounced among small and medium-sized enterprises (SMEs), which often operate on tight budgets and lack access to specialized cybersecurity personnel. Employee-related challenges, such as low awareness (14.8%) and weak management support (7.5%), further compound the problem by preventing a culture of cybersecurity from taking root within organizations.

These findings point to the need for a multi-dimensional response. Firstly, there must be a greater emphasis on capacity building, particularly in cybersecurity training programs that target both technical staff and general employees. Secondly, government support and incentives—such as tax reliefs for cybersecurity investments or subsidized training programs—can ease the financial burden on SMEs. Thirdly, regulatory frameworks should be strengthened to ensure minimum security standards, especially in sectors that manage sensitive or financial data.

Finally, fostering public-private partnerships can accelerate the dissemination of best practices and technologies. As Tambo and Adesina (2022) suggest, sustainable digital transformation in Africa hinges not only on technology deployment but also on institutional readiness, stakeholder collaboration, and culturally aligned policy frameworks.

5.0 Conclusion

This study investigated the level of cybersecurity awareness, the extent of cybersecurity measure adoption, and the challenges faced by businesses in Nigeria in implementing robust security

frameworks. The results revealed that while a moderate level of awareness exists, comprehensive understanding and strategic implementation of advanced cybersecurity practices remain limited. Most businesses have adopted basic protective tools like antivirus software, but critical measures such as multi-factor authentication and employee training are significantly underutilized. The primary barriers identified include a lack of technical expertise, financial constraints, and limited institutional support. These findings indicate that Nigerian businesses, particularly SMEs, are still in the early stages of cybersecurity maturity and remain highly vulnerable to emerging threats. Bridging these gaps requires targeted interventions that address both capacity limitations and structural barriers, while fostering a culture of proactive cyber risk management.

5.1 Recommendations

Invest in Cybersecurity Training and Capacity Building

One of the most critical needs identified in this study is the lack of technical expertise and awareness across business sectors. Therefore, both private enterprises and public institutions should prioritize ongoing cybersecurity training programs for employees at all levels. Specialized workshops, certifications, and online courses can empower staff with the knowledge required to detect and respond to cyber threats effectively. Government agencies, in collaboration with industry stakeholders, can develop national cybersecurity skill-building initiatives targeting SMEs and startups. This will not only improve awareness but also build a sustainable talent pipeline for the growing cybersecurity demands in Nigeria.

Strengthen Government Support and Incentivize Adoption

To mitigate financial and infrastructural challenges, the government should play a more proactive role by offering incentives for cybersecurity investments. These may include tax rebates for businesses that implement industry-standard security protocols, subsidies for SMEs purchasing cybersecurity solutions, and grants for innovative security projects. Furthermore, the establishment of public-private partnerships can facilitate the sharing of best practices and resources. Regulatory bodies should also enforce minimum cybersecurity standards across all business sectors to drive compliance and resilience in the national digital ecosystem.

Promote a Culture of Cybersecurity at the Organizational Level

Organizational leadership plays a pivotal role in driving cybersecurity adoption. Companies should embed cybersecurity into their strategic planning and daily operations, with clear policies, monitoring systems, and accountability structures. Management must be actively involved in promoting a security-conscious work environment by encouraging best practices such as secure password use, regular system audits, and prompt reporting of suspicious activities. By fostering a culture of cybersecurity from the top down, businesses can shift from a reactive approach to one that is preventive and strategic, thus reducing their vulnerability to cyber threats.

References

Businessday NG. (2023). *Securing the future: Aligning cybersecurity with Nigeria's digital revolution*.

Ejeofobiri, C. (2023). *Leveraging artificial intelligence to enhance cybersecurity learning and awareness in Nigeria*. Vanguard.

Independent Newspaper Nigeria. (2023). *Nigerian economy: Digital revolution and cybersecurity*.

ISSAN. (2024). *Nigeria must launch national awareness campaigns to combat rising cybercrime*. *The Guardian Nigeria News*.

Okoye, C., & Eze, T. (2022). Cybersecurity challenges and awareness among SMEs in Nigeria. *International Journal of Information Security Research, 13*(2), 88–96.

Olatunji, A. (2023). *The role of artificial intelligence in enhancing cybersecurity awareness for Nigerian public and private organizations*. *Tribune Online*.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2023). Cybersecurity awareness and challenges in developing economies: A regional perspective. *Journal of Cyber Policy and Management, 8*(1), 45–62. https://doi.org/10.1080/xyz123456

Tambo, E., & Adesina, O. (2022). Building cyber-resilience in African digital ecosystems: Policy and capacity development perspectives. *African Journal of Information Systems, 14*(3), 233–247.

The Firma Law Practice. (2023). *Cybersecurity legal toolkit for businesses in Nigeria*.