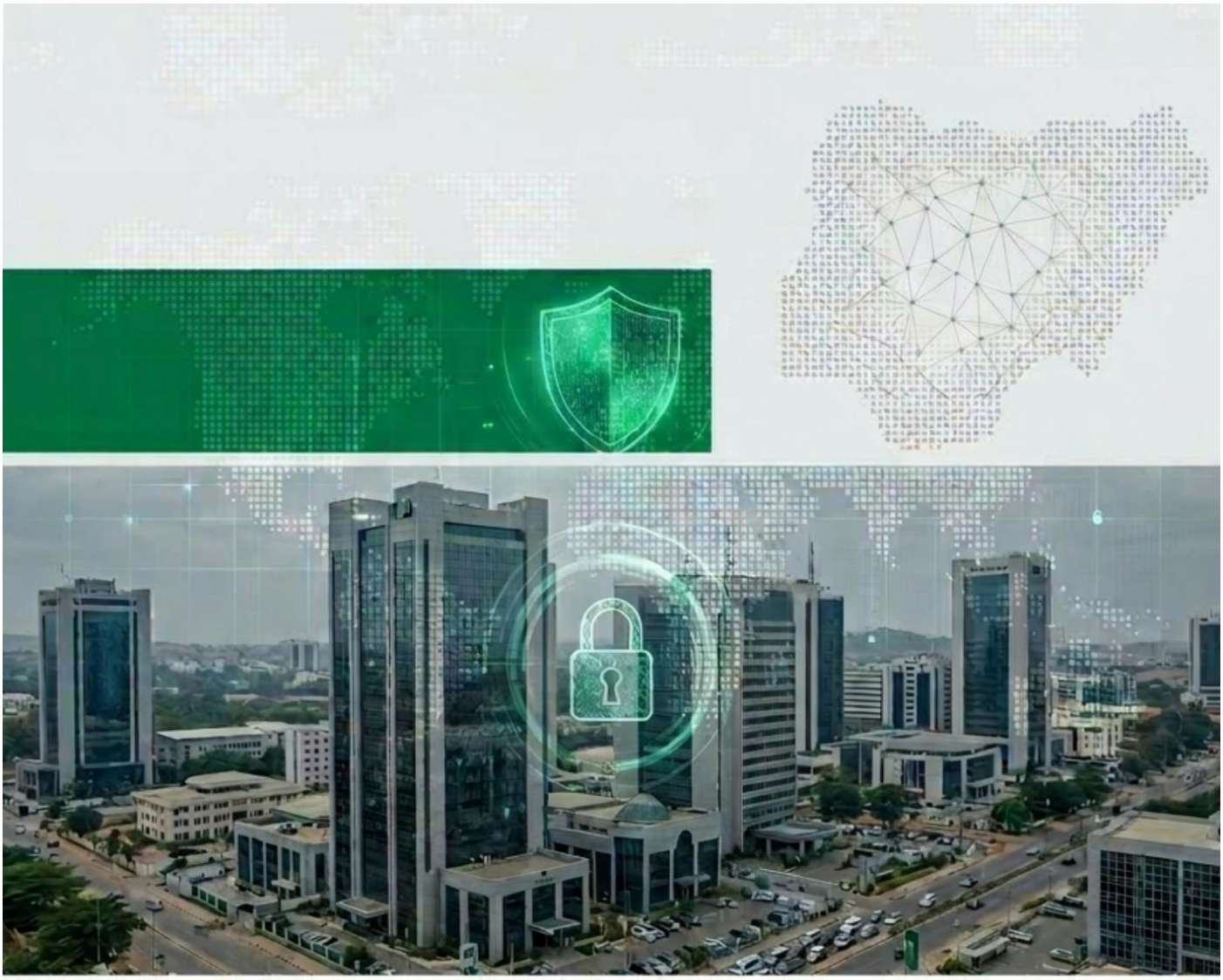


Cyber Risk Insights for Nigerian SMEs

PRACTICAL STRATEGIES FOR RISK COMMUNICATION AND GOVERNANCE

By: **Terdoofan Agber**

MARCH 2026

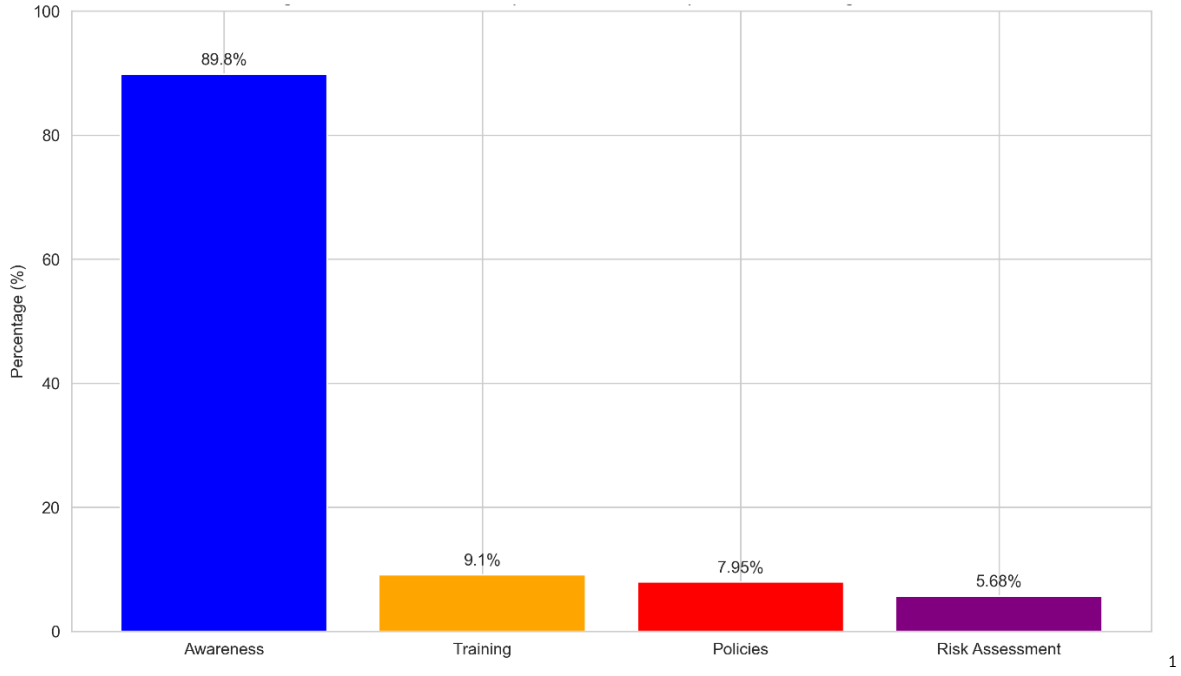
Executive Summary

Nigerian Small and Medium-sized Enterprises (SMEs) are at a critical crossroads. As the backbone of the economy employing about 84% of the workforce, approximately 96% of all businesses and driving innovation across various sectors, these enterprises are simultaneously experiencing an unprecedented surge in cyber threats while lacking the resources and expertise to defend themselves effectively (Falowo et al., 2022; Musabayana et al., 2023). This report provides comprehensive insights into the current cybersecurity crisis facing Nigerian SMEs and offers practical, actionable strategies for improving risk communication and governance.

The Crisis is Quantifiable and Escalating

Recent data from 2025 paints a troubling picture. Nigeria recorded over 119,000 data breaches in the first quarter of 2025 alone, ranking the country among the top ten globally for cyber incidents (Profiled Nigeria, 2025). The first half of 2025 saw 1.46 million cyber-attack attempts blocked, while 2024 witnessed a 150% surge in AI-driven attacks on Nigeria's financial sector (Deloitte, 2025). Compounding these concerns, more than 60 million Nigerian records have been reportedly put for sale on the dark web (CYFIRMA, 2025). The economic impact is staggering, with an estimated ₦288 billion ($800 million) drained annually from Nigeria's economy by cybercrime, and African businesses losing over $4 billion annually (Serianu, 2023).

Figure 1: The Readiness Gap: Awareness vs. Implementation in Nigerian SMEs



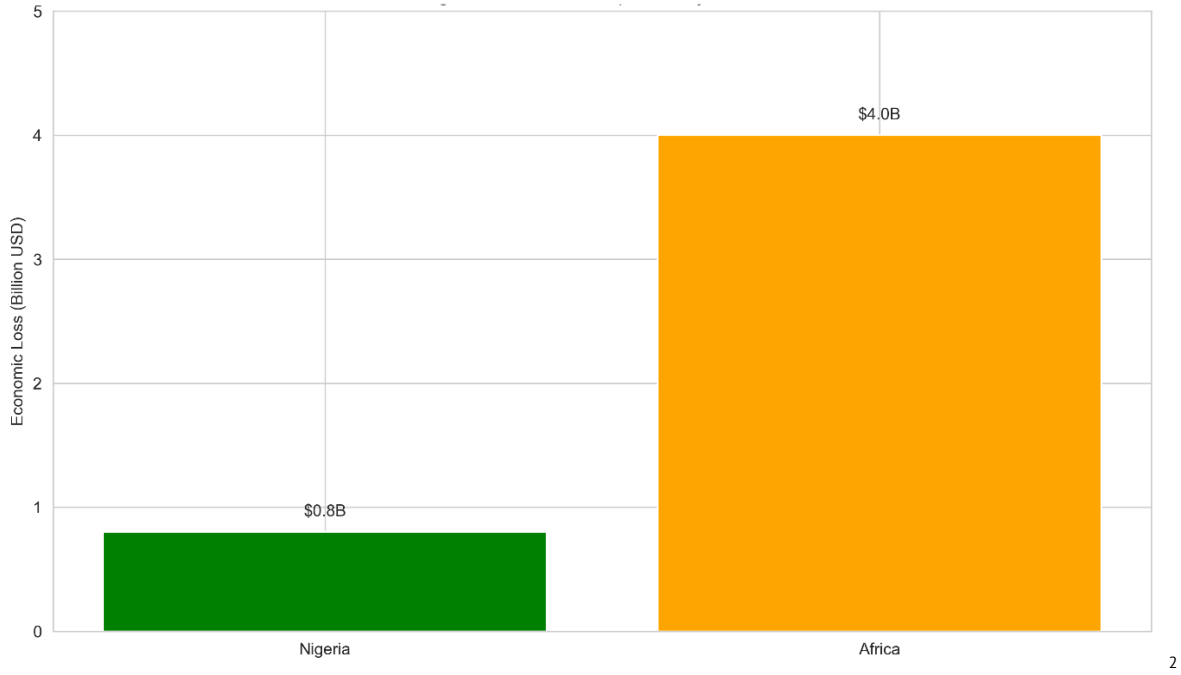
The Readiness Gap Remains Alarming

A comprehensive 2025 study conducted in Edo State reveals what researchers term the "awareness-action gap." While 89.8 % of SMEs are aware of cybersecurity, implementation remains critically low. Only 9.1 % of SMEs have received formal cybersecurity training, a mere 7.95 % have written cybersecurity policies, and just 5.68 % conduct regular risk assessments

[1] Figure 1 illustrates the *awareness-action gap* identified by Pereye et al. (2025). While 89.9% of SMEs demonstrate awareness of cybersecurity, implementation of fundamental protective measures remains critically low, with fewer than 10% conducting training, maintaining written policies, or performing regular risk assessments.

(Pereye et al., 2025). The study found that 36.36 % of SMEs experienced at least one cybersecurity incident, with phishing identified as the most critical vulnerability by 89.8 % of respondents. This vulnerability stems from the absence of practical guidance, the lack of a simplified national cybersecurity baseline, and the dangerous misconception that small businesses are too insignificant to be targeted (Junior et al., 2023).

Figure 2: Economic Impact of Cybercrime on Nigerian and African Economies



[2]

What This Report Provides

This report offers a comprehensive analysis of the Nigerian SME cyber threat landscape, drawing on some of the latest research and statistical data available (Benjamin et al., 2024; Reis et al., 2024). It presents evidence-based governance and risk communication strategies specifically adapted to Nigerian contexts, acknowledging the unique cultural, infrastructural, and resource challenges that local SMEs face (Chaudhary et al., 2023; Corradini, 2020). It also includes a practical, phased implementation roadmap for SME owners and managers, along with strategic policy recommendations for the Nigerian government and regulators. Throughout, the focus remains on cost-effective approaches that respect the resource constraints typical of small and medium enterprises (Shojaifar & Fricker, 2023).

Key Recommendations

For SMEs, the recommended approach begins with immediate, low-cost protections. Every business should implement multi-factor authentication on all critical accounts, establish regular automated backups stored separately from primary systems, and conduct basic cybersecurity awareness sessions for all staff (CISA, 2023). These foundational steps should be followed by the gradual development of formalised governance structures, including documented policies, assigned roles and responsibilities, and regular risk assessments (NIST, 2018). For policymakers, the recommendations are more structural. There is an urgent need to establish dedicated SME cybersecurity support infrastructure, create economic incentives for

[2] Figure 2 compares the annual economic impact of cybercrime on Nigeria (₦288 billion / $800 million) against the broader African context ($4 billion total). Data compiled from Serianu (2023) and Profiled Nigeria (2025) demonstrate that Nigeria represents a significant portion of the continent's cybercrime losses.

security investment, and develop simplified compliance frameworks that acknowledge the limited resources of smaller businesses (Ardo et al., 2023; Oyedeji et al., 2024). Building national capacity through education, training, and public-private partnerships is equally essential.

The Stakes are National

Securing Nigeria's SME sector is not merely a business imperative but a matter of economic and national security (Ibrahim et al., 2024). A collaborative, multi-stakeholder approach can transform Nigeria's cybersecurity posture from a position of vulnerability into a competitive advantage in the global digital economy. This vision is achievable, but it requires commitment, investment, and sustained effort from all stakeholders. The alternative - continued vulnerability and escalating losses - is far costlier.

Table of Contents

1.0 Introduction

The global cyber threat landscape is characterised by diverse and evolving threats, including malware, ransomware, phishing, denial-of-service attacks, and the exploitation of unpatched vulnerabilities (Falowo et al., 2022). Cybercriminals increasingly target government agencies, high-tech companies, and entire economic sectors with the intent of causing disruption, stealing sensitive information, and/or achieving financial gain. This global trend has significant implications for developing economies where digital transformation is accelerating but cybersecurity capacity often lags behind (Akpan et al., 2020). In Nigeria, cybercrime presents a particularly complex challenge. The country has gained international recognition as a source of various online frauds, with the term *419 fraud* referring to the section of the Nigerian Criminal Code dealing with fraudulent offences (Lazarus & Button, 2022). The digital form of this fraud, known locally as *Yahoo-Yahoo*, predominantly involves young, even university-educated men who target victims worldwide (Lazarus & Button, 2022). This reputation creates a paradoxical situation where legitimate Nigerian businesses face heightened international scrutiny while simultaneously being targeted by sophisticated criminal networks operating both within and outside the country.

The significance of cybersecurity for Nigerian SMEs cannot be overstated. These enterprises form the backbone of the national economy, employing a substantial portion of the workforce and driving innovation across multiple sectors (Musabayana et al., 2023). According to the Small and Medium Enterprises Development Agency of Nigeria, SMEs account for approximately 96% of businesses and 84% of employment in the country (SMEDAN, 2022). A well-supported SME sector can generate positive economic outcomes, including job creation, wealth distribution, and sustainable development. However, the cybersecurity challenges facing these businesses threaten to undermine these benefits. Cyber attacks can lead to immediate financial losses, long-term reputational damage, and severe operational disruptions that many small businesses struggle to survive (Okundaye et al., 2019).

To address these challenges, Nigerian SMEs must adopt cybersecurity measures that go beyond simple technical solutions. Effective protection requires comprehensive employee training, secure ICT infrastructure, and consistent adherence to established best practices for information security management (Benjamin et al., 2024). Equally important is the role of government in supporting SMEs through policies and initiatives that enhance cybersecurity awareness and resilience across the sector (Abdul-Azeez et al., 2024).

2.0 The Cybersecurity Imperative for Nigerian SMEs

2.1 Nigeria's Digital Transformation Journey

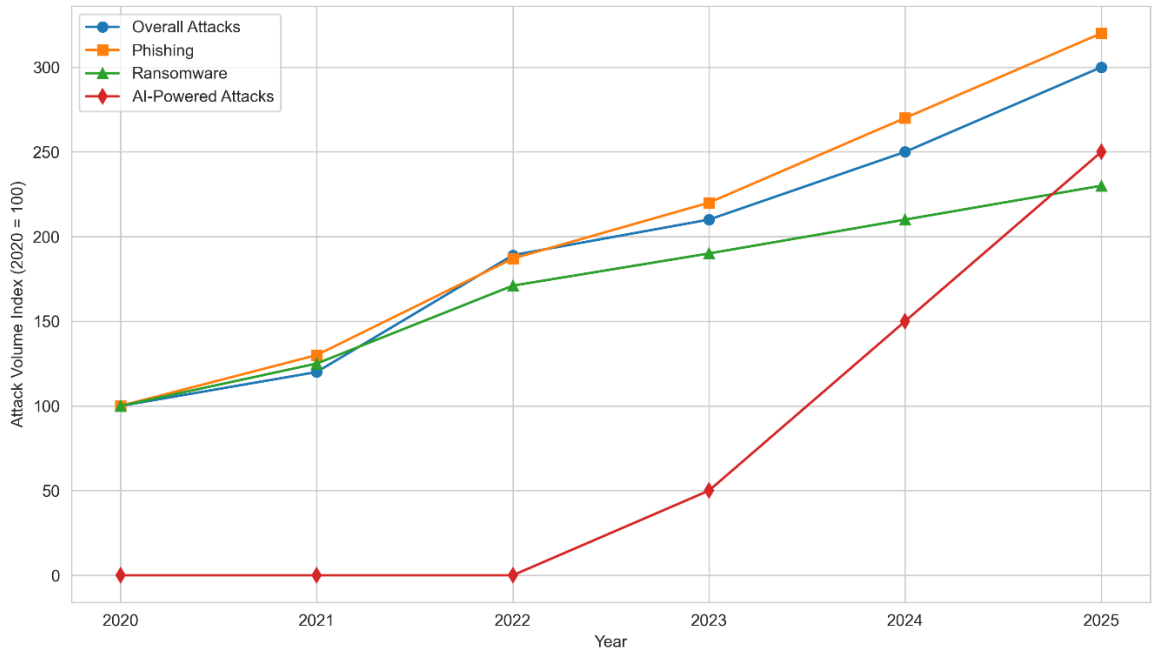
Nigeria is undergoing a major digital transformation that promises immense economic opportunity. The COVID-19 pandemic dramatically accelerated the adoption of digital technologies across all sectors, with SMEs rapidly embracing e-commerce platforms, mobile banking, fintech solutions, and cloud-based services (Akpan et al., 2020). According to the Nigerian Communications Commission (NCC), internet penetration reached 55.4% of the population by 2023, with mobile subscriptions exceeding 220 million (NCC, 2023). This digital revolution has enabled businesses to reach new customers, streamline operations, and participate in the global digital economy in ways that were previously unimaginable for enterprises of that scale.

However, this digital revolution has also exponentially expanded the attack surface available to cybercriminals by creating vulnerabilities that threaten individual businesses and the broader economy. The rapid digitisation brought on by the pandemic left many SMEs with insufficient cybersecurity planning, thereby exposing them to malicious actors (Haastrecht et al., 2021). A major challenge facing SMEs in developing economies is the limited access to and adoption of state-of-the-art technologies (Akpan et al., 2020). This technological gap leaves SMEs particularly vulnerable to cyber threats, as they struggle to keep pace with rapidly evolving cybersecurity developments (Ewuga et al., 2023).

2.2 The Growing Threat Landscape

Recent data reveals an alarming escalation in cyber threats targeting Nigerian businesses. In 2022, Nigerian SMEs experienced an 89% surge in overall cyber attacks compared to the previous year (Guardian Nigeria, 2022). Phishing attacks specifically increased by 87% during the same period, demonstrating the growing sophistication of social engineering tactics (Nairametrics, 2023). Ransomware also emerged as a particularly severe threat, with about 71% of Nigerian firms experiencing such attacks in 2021, significantly above the 66% global average (VPN Alert, 2026). The financial consequences are severe with the average cost to recover from a ransomware attack reaching $3.43 million, representing a staggering 644% year-over-year increase (Nairametrics, 2023).

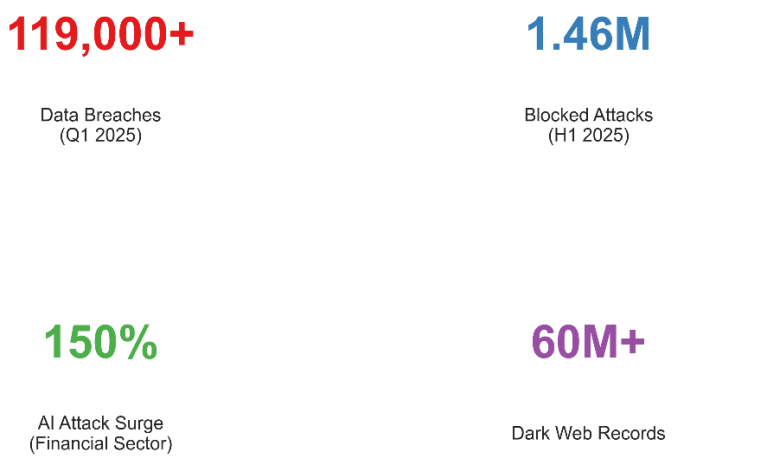
Figure 3: Growth Trends in Cyber Threats Targeting Nigerian SMEs (2020-2025)



[3]

[3] Figure 3 illustrates the accelerating trajectory of cyber threats in Nigeria from 2020 to 2025. The sharp upward trend in overall attacks, combined with the dramatic 87 % surge in phishing (Nairametrics, 2023) and the emergence of AI-powered attacks (Deloitte, 2025), demonstrates the rapidly evolving threat landscape facing SMEs.

Figure 4: 2025 Threat Metrics Dashboard

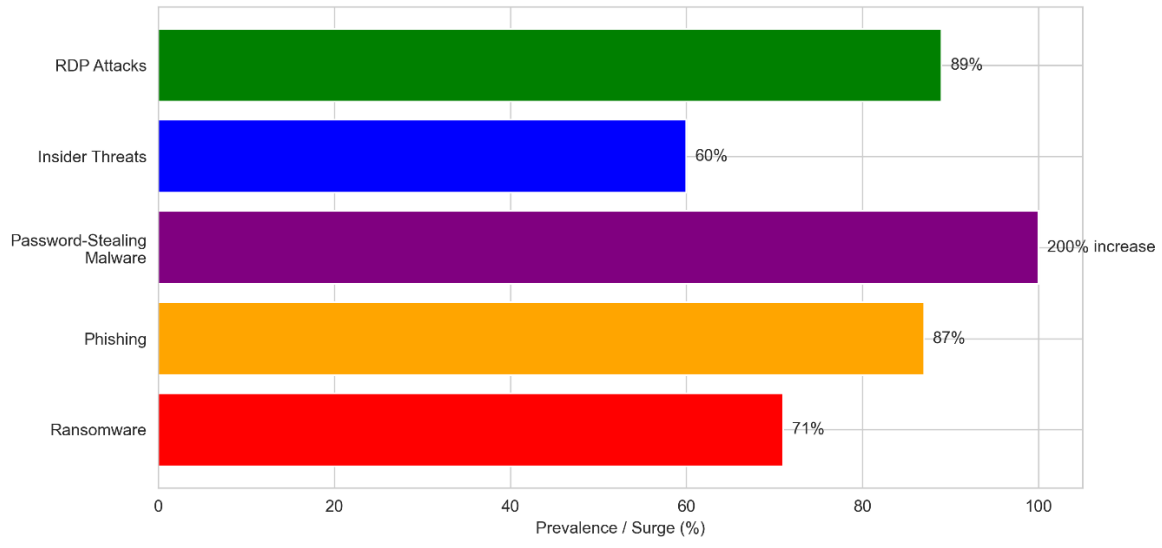


[4]

2.3 Key Threat Vectors

Ransomware remains one of the most destructive threats facing Nigerian SMEs. This malicious software encrypts business data and demands payment for decryption keys, often crippling operations for weeks or months (VPN Alert, 2026). According to research by Carias et al. (2020), the impact extends far beyond the ransom payment itself to include operational downtime, reputational damage, and substantial recovery costs. SMEs are particularly vulnerable to these attacks because they frequently lack the backup systems and incident response capabilities that larger organisations maintain (Haastrecht et al., 2021).

Figure 5: Primary Threat Vectors Affecting Nigerian SMEs



[5]

Source: Compiled from Benjamin et al., 2024; Haastrecht et al., 2021; VPN Alert, 2026

[4] Figure 4 presents a dashboard of key 2025 threat metrics. The data reveals multiple simultaneous crises: massive data breaches, unprecedented attack volumes, the emergence of AI-powered threats, and widespread exposure of Nigerian records on dark web marketplaces (Profiled Nigeria, 2025; CYFIRMA, 2025; Deloitte, 2025).

[5] Figure 5 provides a visual overview of the primary threat vectors facing Nigerian SMEs, with impact levels and prevalence rates indicated. Ransomware affects 71 % of firms (VPN Alert, 2026), while phishing attacks surged by 87 % in 2022 alone (Nairametrics, 2023).

Phishing attacks continue to evolve in sophistication and prevalence. These fraudulent emails, messages, or websites are designed to steal credentials or install malware, exploiting human psychology rather than technical vulnerabilities (Benjamin et al., 2024). These attacks are particularly effective when employees lack security awareness training and cannot recognise the subtle indicators of fraudulent communications. The 87% surge in phishing attacks targeting SMEs in 2022 demonstrates the growing effectiveness of social engineering tactics against under-prepared organisations (Nairametrics, 2023). Password-stealing malware, often delivered through trojans that capture login credentials for banking, email, and business systems, has seen detections more than double in recent years (Guardian Nigeria, 2022). These attacks specifically target SMEs because they often lack advanced threat detection capabilities and may not have implemented even such basic protections as multi-factor authentication (Shojaifar & Fricker, 2023).

Insider threats, whether malicious or accidental, represent a significant and often overlooked threat vector. Security risks posed by employees, contractors, or business partners who have authorised access but use it maliciously or negligently can be particularly damaging due to the trusted nature of their access (Haastrecht et al., 2021). Whether through deliberate data theft or accidental exposure, insider incidents often evade traditional security controls designed to detect external threats. Remote Desktop Protocol attacks increased by 89% as remote work proliferated during the COVID-19 pandemic. Attacks targeting poorly secured remote access systems grew from 161,000 incidents to over 303,500, highlighting the risks associated with rapid adoption of remote work technologies without adequate security controls (Guardian Nigeria, 2022). SMEs adopting hybrid work models remain particularly vulnerable to these attacks.

2.4 Why SMEs are Targeted

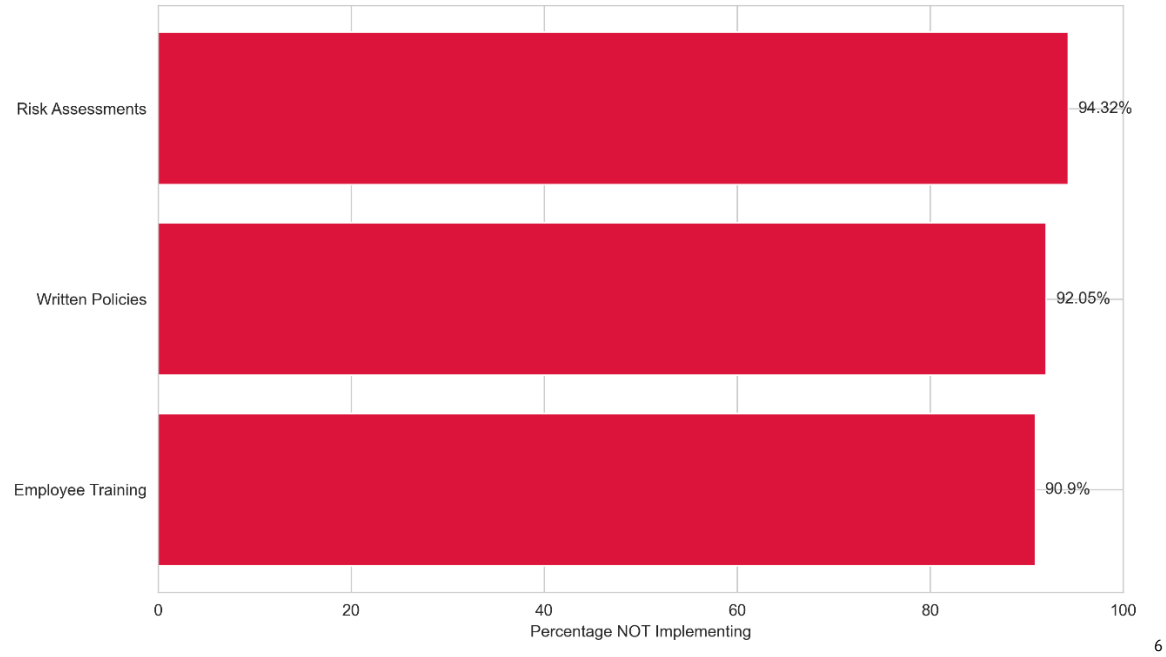
A dangerous myth persists among many small business owners - the belief that their businesses are too small to attract the attention of cybercriminals. Junior et al. (2023) found that this misconception is widespread and significantly contributes to inadequate defences. The reality, though, is fundamentally different. SMEs are deliberately targeted because they typically have weaker defences yet possess valuable data including customer information, financial records, and intellectual property (Kandpal et al., 2023). Additionally, they often serve as entry points to larger corporate partners through supply chain relationships, making them attractive targets for attackers seeking access to more secure organisations (Foli et al., 2022). Several interconnected factors contribute to the vulnerability of Nigerian SMEs.

Resource constraints, including limited financial and human capital, restrict investment in the necessary security measures as many SMEs operate under tight budgets that force reliance on less effective, cost-constrained solutions rather than comprehensive security programmes (Junior et al., 2023). The cybersecurity literacy gap is equally significant. Many SME leaders and employees lack fundamental understanding of cyber threats and protective measures, creating exploitable human vulnerabilities that technical controls alone cannot address (Chaudhary et al., 2023). There is also the challenge of Nigerian businesses struggling with basic cybersecurity practices due to infrastructural limitations and limited access to affordable solutions (Ewuga et al., 2023). The lack of cybersecurity literacy and financial resources renders these enterprises particularly vulnerable to attacks that more mature organisations would easily repel. Unfortunately, Nigeria's international reputation for cybercrime further creates a paradoxical situation where legitimate SMEs face heightened scrutiny while being targeted by sophisticated criminal networks (Lazarus & Button, 2022).

2.5 The Readiness Gap

Research conducted among SMEs in Edo State reveals a deeply troubling picture of preparedness. According to the International Journal of Scientific Research and Analysis (Pereye et al., 2025), 90.9% of SMEs have never provided cybersecurity training to their employees. An even more striking 92.05% operate without written cybersecurity policies, meaning that security decisions are made reactively and inconsistently. Perhaps most concerning from the study is that about 94.32% do not conduct regular risk assessments, leaving them unable to identify and prioritise their most significant vulnerabilities.

Figure 6: SME Preparedness: Percentage NOT Implementing Security Practices

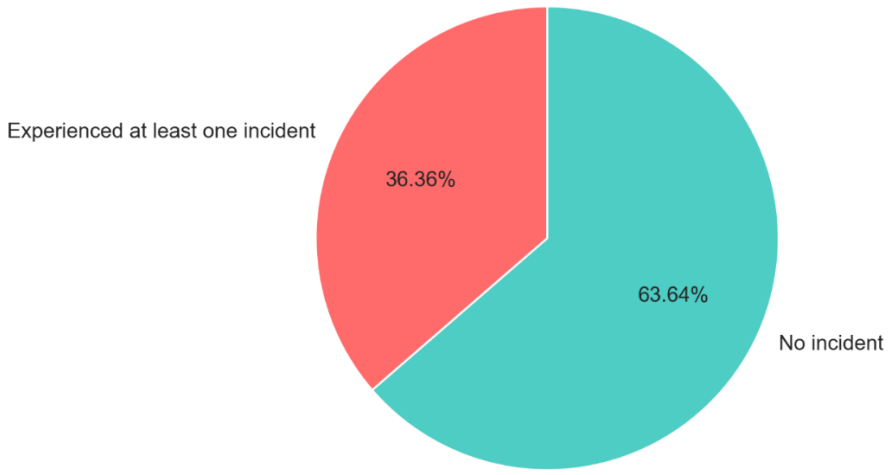


Source: Pereye et al., 2025; IJSRA, 2025

These findings align with broader research on SME cybersecurity in developing economies. Junior et al. (2023) conducted a systematic review of SME cybersecurity and found that resource constraints, lack of expertise, and inadequate awareness are consistent themes across multiple countries and contexts. The lack of cybersecurity literacy among SME personnel contributes significantly to their vulnerability, as many employees genuinely believe their organisations are too small to be targeted, leading to inadequate defences and risky behaviours (Kandpal et al., 2023).

[6] Figure 6 illustrates the fundamental gaps in SME preparedness, with over 90 % of organisations failing to implement basic security practices. The data reveals that the majority of SMEs operate without designated security personnel or incident response capabilities, leaving them dangerously exposed to cyber threats.

Figure 7: SME Incident Experience



[7]

Source: Pereye et al., 2025

This combination of limited resources, inadequate knowledge, and misplaced confidence creates an environment where cyber threats can thrive, posing significant risks to the operational integrity of Nigerian SMEs.

[7] Figure 7 shows that more than one in three SMEs have experienced at least one cybersecurity incident, demonstrating that this is not a theoretical risk but a lived reality for a substantial portion of the sector.

3.0 The Governance and Risk Communication Challenge

3.1 Beyond Technology

The belief that cybersecurity is fundamentally a technology problem solvable through the purchase and deployment of expensive security software is one that has proved harmful to the cyber resilience of small businesses (Corradini, 2020). While technology is essential, research has consistently demonstrated that the most significant vulnerabilities are organisational in nature, rooted in poor governance, unclear accountability, and ineffective communication rather than technical deficiencies alone (Sutton & Tompson, 2023).

For Nigerian SMEs, effective governance translates directly to positive business outcomes. It enhances customer trust by demonstrating that the organisation takes data protection seriously and improves operational resilience by ensuring that security considerations are integrated into business processes rather than treated as afterthoughts (Abdul-Azeez et al., 2024; Carias et al., 2020). It facilitates regulatory compliance with frameworks such as the Nigeria Data Protection Act (NDPA), reducing legal and financial risks (Ardo et al., 2023) and very importantly, also creates a competitive advantage when SMEs pursue enterprise clients or international partnerships that require demonstrated security capabilities.

Effective governance ensures that security priorities are fully integrated with business objectives, rather than being treated as a competing interest. According to Oluokun et al. (2024), this alignment allows for responsibilities to be clearly assigned across the organisation, which eliminates the confusion that typically leads to security gaps. Instead of relying on arbitrary budgets, resources can be allocated systematically based on actual risk priorities. This shift moves the business away from reactive fixes and towards a model where risks are identified and managed before they escalate. Consequently, when incidents do occur, they are handled through established procedures rather than improvised responses, allowing for timely detection and reporting. This structured approach also creates a cycle of continuous improvement, ensuring that security practices evolve to meet emerging threats rather than becoming static or obsolete.

3.2 Structural Governance Deficiencies

Unclear accountability is perhaps the most fundamental governance deficiency in Nigerian SMEs. Without designated security officers or teams, responsibility for cybersecurity is often spread too thinly across the organisation or left entirely unassigned (Neri et al., 2023). This lack of leadership means that when an incident occurs, there is no one to coordinate the response, make critical decisions, or communicate with stakeholders. Such a diffusion of responsibility leads to delayed actions, inconsistent security practices, and a culture of finger-pointing rather than practical problem-solving. This issue is further compounded by the reactive posture many businesses adopt. According to Carias et al. (2020), organisations operating in this mode only address security after a breach has occurred, focusing on immediate damage control rather than long-term prevention. This approach is not only more expensive but also less effective than proactive risk management. For many SMEs lacking the necessary resources or expertise, this remains the default setting, creating a vicious cycle. Limited resources are consumed by responding to avoidable incidents, leaving even less available for preventive measures, which inevitably leads to further breaches.

Framework adoption barriers further complicate the governance landscape. International cybersecurity frameworks such as NIST, ISO 27001, and COBIT represent the gold standard for enterprise security governance (Özkan & Spruit, 2020).

However, their complexity, resource requirements, and enterprise focus create significant adoption barriers for SMEs in developing economies. Business owners and managers faced with hundreds of pages of detailed controls and requirements often experience confusion, leading to ineffective implementation and, in many cases, complete abandonment of structured governance approaches (Perozzo et al., 2022).

3.3 Risk Communication and Cultural Challenges

The knowledge-action gap represents a persistent challenge in cybersecurity communication. Many awareness campaigns successfully impart knowledge about threats and protective measures, but this knowledge frequently fails to translate into consistent, secure behaviours (Khan & Muntaha, 2024). This gap persists because training content often lacks relevance to employees' actual work contexts, one-time sessions create only temporary awareness that quickly fades, technical jargon alienates non-technical staff, consequences seem abstract and unlikely, and secure behaviours are perceived as inconvenient impediments to productivity (Corradini, 2020).

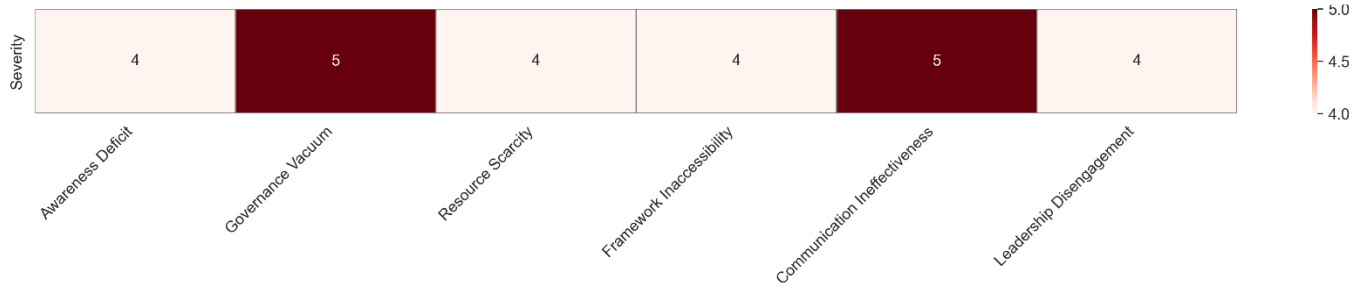
Leadership involvement is the single most critical factor in bridging this gap. When senior management visibly prioritises security through their words and actions, employees perceive cybersecurity as organisationally important and adjust their behaviours accordingly (Antunes et al., 2022). Conversely, when leadership relegates security to an *IT problem* and demonstrates through their actions that security is secondary to other concerns, security initiatives languish regardless of how well they are designed or communicated.

Nigerian cultural factors add additional layers of complexity to risk communication. Effective communication must navigate the country's rich linguistic diversity, with employees speaking different languages and coming from different cultural backgrounds (Kori-Siakpere et al., 2024). Hierarchical organisational structures affect how information flows and who feels empowered to raise security concerns. Infrastructure constraints limit the communication channels available, particularly for SMEs operating outside major urban centres. Cultural communication norms, including preferences for oral rather than written communication and the importance of personal relationships in business contexts, must be understood and accommodated for security messages to resonate effectively (Iguodala-Cole, 2024).

3.4 Critical Gaps Identified

The governance and risk communication gaps in Nigerian SMEs often start with a basic lack of cybersecurity awareness among both management and staff. This problem is made worse by a lack of formal oversight where responsibilities and decision-making processes are rarely defined. Because of this, many business leaders tend to view security as a technical IT issue rather than a core business priority that requires their direct involvement.

Figure 8: Heatmap of Critical Cybersecurity Gaps



[8]

Source: Analysis based on research findings

These organisations also face significant practical hurdles regarding limited budgets and a shortage of skilled personnel to manage security. Many find international cybersecurity standards too complex or expensive to adopt, leaving them without a clear framework to follow. Even when training is provided, it often fails to change actual behaviour because the communication styles used do not always suit the local Nigerian contexts or the specific linguistic needs of the workforce.

Table 1: Summary of Identified Governance Gaps and Challenges

Gap	Description	Consequence
Awareness Deficit	Lack of cybersecurity literacy	Employees cannot identify threats
Governance Vacuum	No clear accountability	Delayed incident response
Resource Scarcity	Limited financial/human capital	Inadequate security investment
Framework Inaccessibility	Standards too complex	Framework abandonment
Communication Ineffectiveness	Knowledge-action gap	Training doesn't change behaviour
Leadership Disengagement	Security relegated to IT	No strategic priority

[8] Figure 8 presents a heatmap visualisation of the severity of critical cybersecurity gaps identified in this research. Governance vacuum and communication ineffectiveness emerge as the most severe deficiencies, followed closely by awareness deficits and resource constraints.

4.0 Framework Adoption and Adaptation

4.1 Adapting International Frameworks

While international frameworks provide valuable structure and recognised standards for cybersecurity governance, Nigerian SMEs require pragmatic adaptation strategies that acknowledge their unique resource constraints and local contexts (Shojaifar & Fricker, 2023). The key to successful framework adoption is selective, phased implementation that prioritises high-impact, cost-effective controls rather than attempting comprehensive compliance from the outset. This approach recognises that a framework partially implemented is far more valuable than a framework abandoned due to complexity or resource demands (Özkan & Spruit, 2020).

4.2 The NIST Cybersecurity Framework

The NIST Cybersecurity Framework (NIST-CSF) provides a practical and accessible starting point for Nigerian SMEs as they begin to develop their security strategies (NIST, 2018). Its flexibility and risk-based approach, combined with the fact that it carries no licensing costs, make it particularly well-suited for organisations operating with limited budgets. The framework is built around five core functions that together offer a comprehensive method for managing cybersecurity risks.

The process begins with the **Identify** function, which helps businesses understand the specific risks facing their systems, assets, and data. This is followed by the **Protect** function, where appropriate safeguards are put in place to ensure that critical services remain operational. To ensure that any breaches are caught early, the **Detect** function focuses on activities that identify security events as they happen. When an incident is discovered, the **Respond** function provides a clear path for taking action, while the **Recover** function ensures that plans are in place to restore normal operations and maintain business resilience.

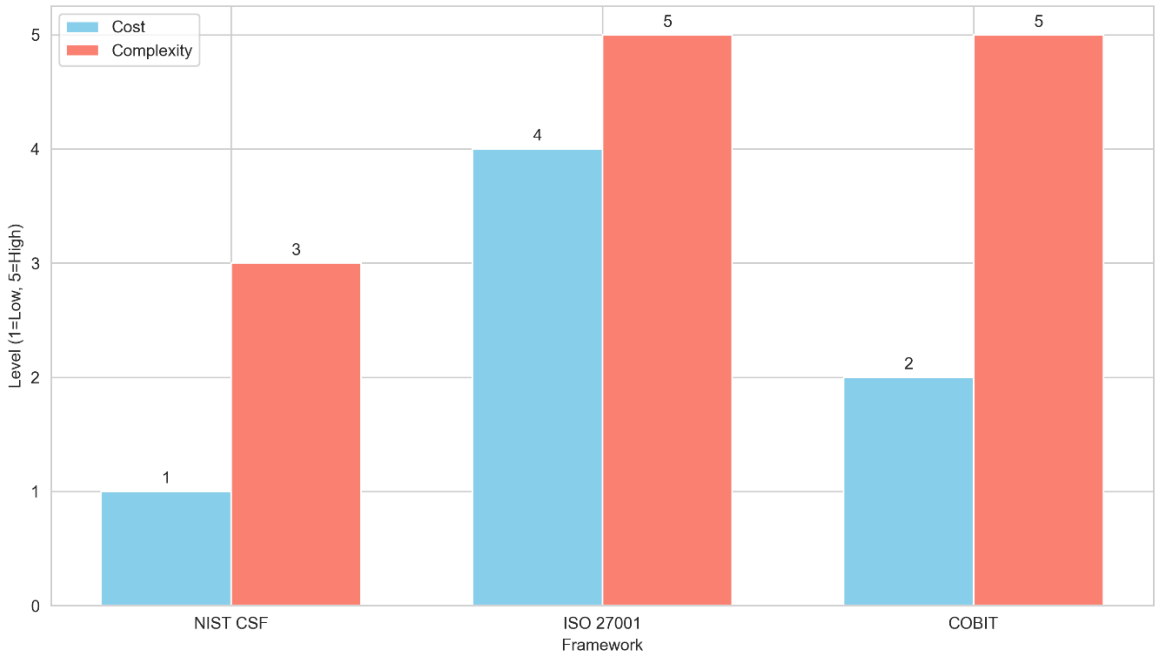
Research by Haastrecht et al. (2021) confirms that the NIST framework's adaptability and scalability make it particularly suitable for SMEs. They note that SMEs can implement the framework by conducting risk assessments to identify their specific vulnerabilities and then prioritising actions based on their unique business context. The framework's emphasis on continuous improvement allows SMEs to gradually enhance their cybersecurity posture as resources permit.

4.3 International Framework Comparison

When comparing available frameworks, each offers distinct advantages depending on an organisation's specific needs and circumstances. According to Shojaifar and Fricker (2023), the NIST-CSF is often the most suitable choice for SMEs starting their security journey due to its medium complexity and the fact that it is free to use. In contrast, ISO 27001 involves higher costs and greater complexity, making it more appropriate for businesses that require international credibility or those pursuing large enterprise clients that mandate certified security systems (Alfaadhel et al., 2023).

COBIT, with its medium cost and high complexity, is best suited to larger, IT-intensive SMEs with mature governance structures and dedicated security personnel (Ogunjimi et al., 2018). Ultimately, the primary challenge for Nigerian SMEs is not necessarily finding the *best* framework in absolute terms. Success lies instead in identifying which specific elements of these frameworks can be practically implemented, given their unique resource constraints and business requirements.

Figure 9: Cybersecurity Framework Comparison for SMEs

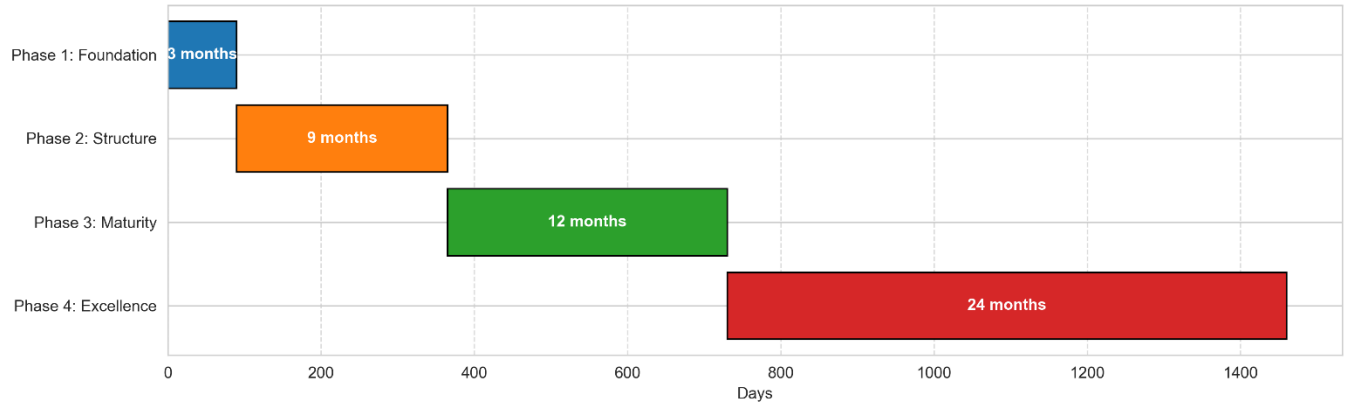


[9]

4.4 Phased Implementation Approach

Rather than attempting comprehensive framework compliance immediately, it is more advisable that SMEs adopt a phased maturity model that builds capability incrementally. This approach is supported by research from Carias et al. (2020) and Sukumar et al. (2023), who advocate for gradual, sustainable implementation.

Figure 10: Phased Cybersecurity Maturity Model for SMEs



[10]

Source: Adapted from Carias et al., 2020; Sukumar et al., 2023

The first phase, spanning the first three months, focuses on essential practices such as multi-factor authentication, regular backups, basic staff training, and the establishment of clear password policies. Once these fundamentals are settled, the

[9] Figure 9 provides a comparative visualisation of the three major cybersecurity frameworks. NIST CSF emerges as the most accessible option for SMEs due to its zero cost and medium complexity, while ISO 27001 and COBIT serve more specific use cases despite their higher barriers to entry (NIST, 2018; ISO/IEC, 2022; Shojaifar & Fricker, 2023).

[10] Figure 10 presents a visual roadmap for phased cybersecurity implementation. Each phase builds on the foundation of the previous phase, ensuring that organisations develop capability progressively rather than attempting ambitious implementations they cannot sustain.

second phase - covering three to twelve months - moves towards formalisation. During this period, the emphasis shifts to documenting policies, assigning specific roles and responsibilities, and developing formal risk assessment and incident response plans.

As the strategy matures into the second year, the third phase focuses on optimisation through continuous monitoring, regular security assessments, and compliance verification. This ensures that the established controls remain effective and relevant. Beyond the two-year mark, the fourth phase aims for excellence. This is where and when the organisation may begin to pursue formal certifications, integrate threat intelligence into its operations, and use industry benchmarking to measure its progress. By following this structured timeline, businesses can manage their security journey in a way that is both practical and sustainable.

4.5 Leveraging Emerging Technologies

Emerging technologies present valuable opportunities for Nigerian SMEs to improve their security in a cost-effective way. Reis et al. (2024) highlights that when offered through cloud-based security services, AI-powered threat detection can provide enterprise-level protection without the need for in-house AI expertise or large capital investments. Similarly, zero-trust architecture can be gradually introduced by implementing strong authentication and access controls, starting with the most critical systems and data before extending to less sensitive areas (Melaku, 2023).

Cloud security services also offer advanced capabilities at prices that suit SMEs, typically through subscription models. This approach removes the need for heavy upfront spending on security infrastructure (Nadella et al., 2024). Additionally, mobile-first security strategies, which include mobile device management and mobile application security, address the widespread use of mobile devices in Nigerian businesses. These strategies prioritise protecting mobile platforms, which are becoming increasingly important in day-to-day operations (Ewuga et al., 2023).

5.0 Research Findings

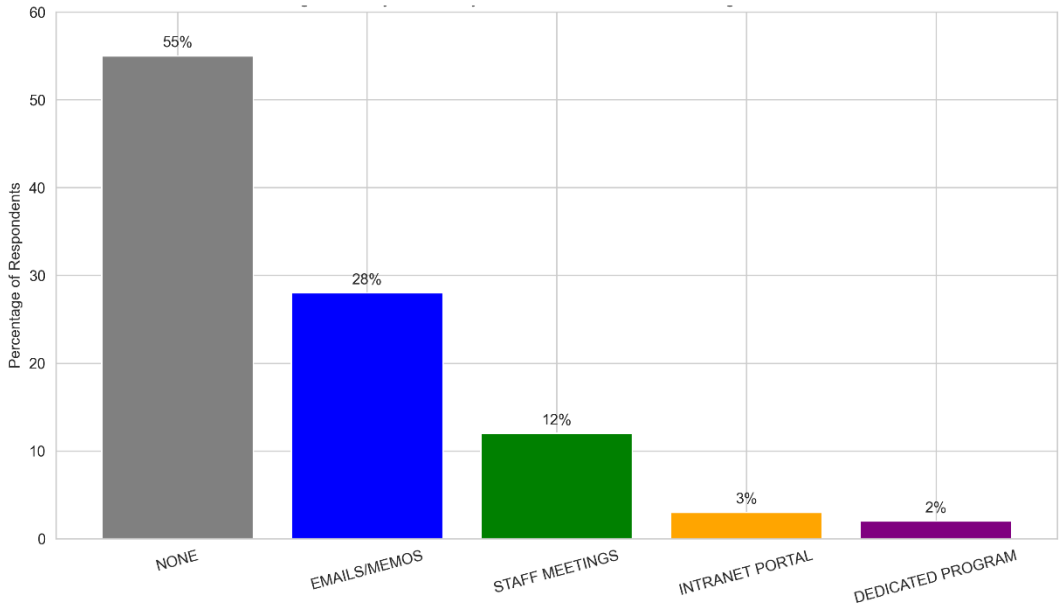
5.1 Methodology

This study employed a mixed-methods approach combining quantitative surveys and qualitative document analysis, following established research practices in cybersecurity studies (Cremer et al., 2022). Surveys were administered to SME owners and managers to assess their cybersecurity awareness, knowledge, and practices. Existing policy documents and previously conducted research provided insights into the challenges and opportunities for enhancing cybersecurity governance. Data collection was conducted through field surveys using questionnaires distributed to selected SMEs, with a total sample size of 106 respondents, consistent with sample sizes in comparable studies (Ogbeide et al., 2023). Python served as the primary programming language for data analysis, with extensive use of Pandas, NumPy, Matplotlib, and Seaborn libraries for data manipulation, statistical analysis, and visualisation.

5.2 Communication Methods and Frequency

The analysis revealed that current communication and awareness efforts are quite limited, relying heavily on informal methods and infrequent updates. A significant number of SMEs lack any formal channels for sharing cybersecurity information, which often leaves staff without clear guidance. Where communication does exist, it typically takes the form of emails, memos, or staff meetings. As Ikuero and Zeng (2022) suggest, this reliance on traditional methods may not be the most effective way to reach all employees or ensure that critical security messages are actually understood and followed.

Figure 11: Cybersecurity Communication Methods in Nigerian SMEs



[11]

Source: Survey data (N=106), 2025

Critically, 55% of respondents indicated that they use no method at all for cybersecurity communication, highlighting a fundamental gap in awareness efforts. Even in organisations where communication does occur, it is often too infrequent to

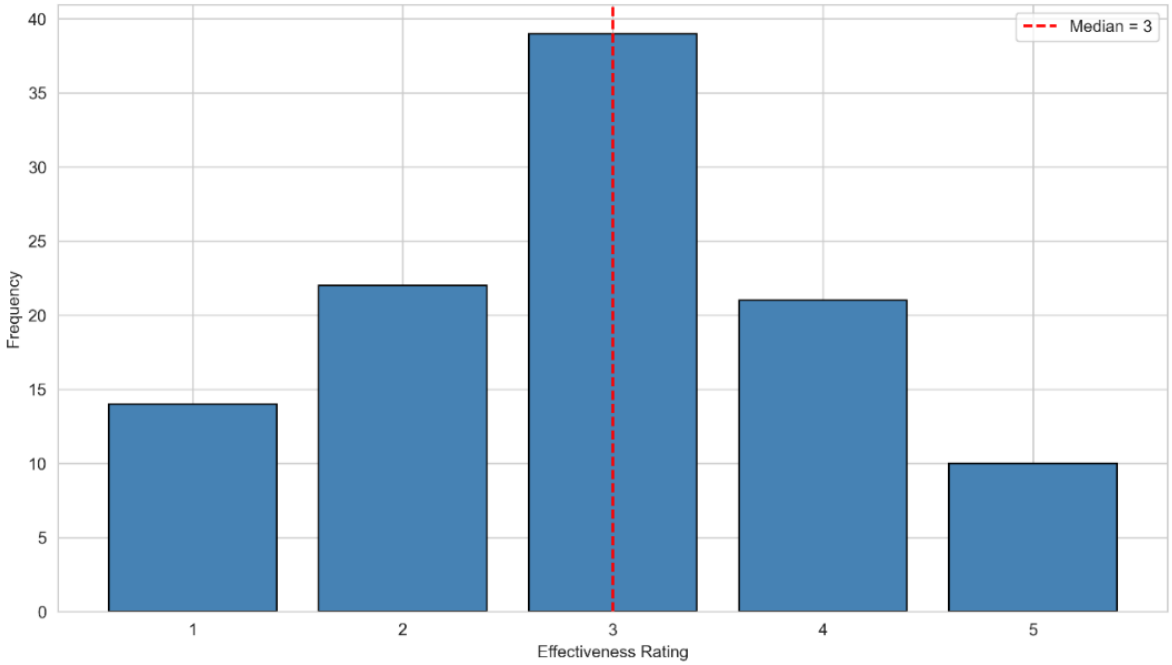
[11] Figure 11 reveals that 55 % of surveyed SMEs use no method at all for cybersecurity communication. Among those who do communicate, reliance on traditional channels such as emails and staff meetings predominates, while structured approaches like dedicated programmes or intranet portals remain rare.

be effective. This lack of regular engagement prevents the development of a proactive cybersecurity culture, where security considerations should be naturally embedded in daily business operations.

5.3 Communication and Governance Effectiveness

The distribution of responses for communication effectiveness leaned towards the lower end of the scale with a median value of 3 out of 5. This indicated that current strategies are perceived as only moderately effective at best, with substantial room for improvement in how security information is conveyed and received (Pereye et al., 2025).

Figure 12: Distribution of Communication Effectiveness Ratings



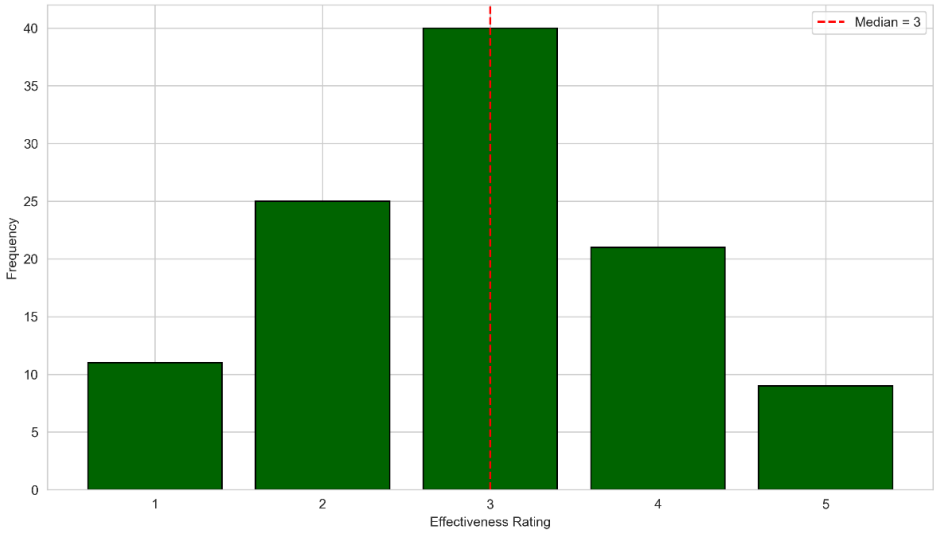
[12]

Source: Author's survey data (N=106), 2025

Similar to communication effectiveness, the perceived effectiveness of governance structures was also skewed towards the lower end with a median of three, suggesting that employees and managers recognise significant gaps in how cybersecurity decisions are made and how accountability for security outcomes is assigned.

[12] Figure 12 shows the distribution of communication effectiveness ratings, with a median of 3 out of 5. The concentration of responses in the mid-range indicates that current strategies are perceived as only moderately effective, with substantial room for improvement.

Figure 13: Distribution of Governance Effectiveness Ratings



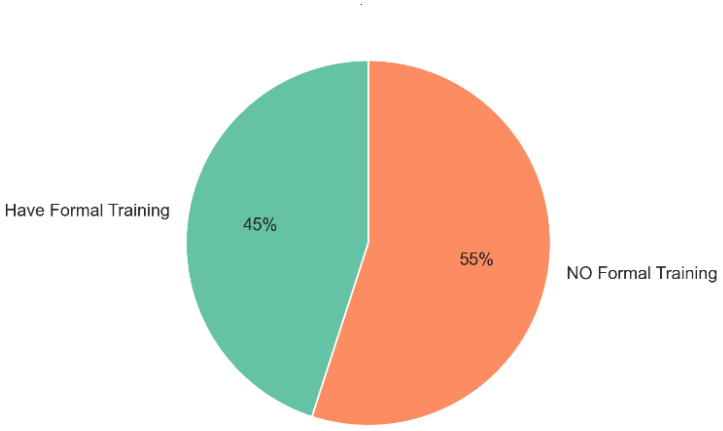
[13]

Source: Author's survey data (N=106), 2025

5.4 Training Programs and Effectiveness

Approximately 55% of organisations have no formal cybersecurity awareness programmes or employee training, representing a critical deficiency in proactive risk mitigation. This finding is consistent with research by Bada and Nurse (2019), who found that SME training programmes are often inadequate or non-existent across developing economies. This finding is particularly concerning given that formal training programmes were significantly associated with higher effectiveness scores in both communication and governance. A moderate positive correlation exists between the presence of training programmes and both communication and governance effectiveness, suggesting that organisations investing in training perceive their communication and governance structures as more effective. This relationship indicates that training can contribute to improved practices, although other factors also play significant roles in determining overall effectiveness.

Figure 14: Organisations with Formal Training Programs



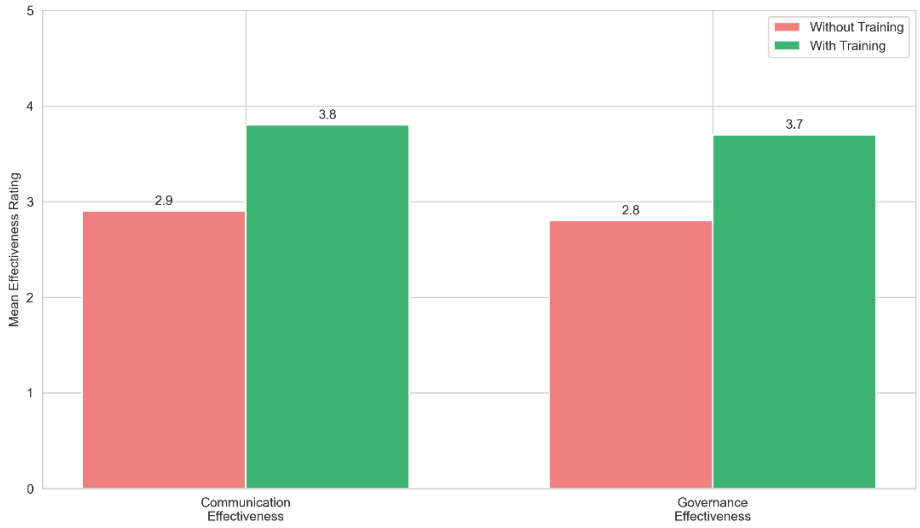
[14]

Source: Author's survey data (N=106), 2025

[13] Figure 13 presents the distribution of governance effectiveness ratings, also with a median of 3. The similarity between communication and governance effectiveness distributions suggests these two dimensions are closely linked, with deficiencies in one area often reflected in the other.

[14] Figure 14 reveals that 55 % of organisations have no formal cybersecurity awareness programmes or employee training, representing a critical deficiency in proactive risk mitigation.

Figure 15: Impact of Training on Communication and Governance Effectiveness



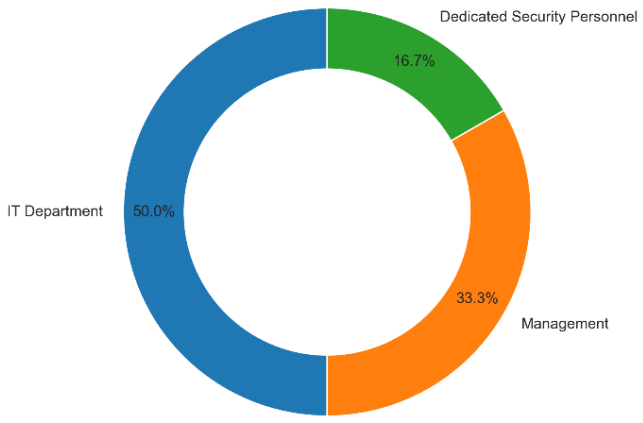
[15]

Source: Author's survey data (N=106), 2025

5.5 Security Responsibility and Risk Assessment

In half of the organisations surveyed, cybersecurity decisions were mainly made by IT departments, while management took the lead in about a third. The limited involvement of dedicated cybersecurity personnel suggested a potential gap in specialised expertise as those making key security decisions may lack the necessary field and technical knowledge (Neri et al., 2023). Furthermore, only 33.3% of SMEs agreed to conducting regular risk assessments, suggesting that many did not have a clear understanding of their cybersecurity risk profile. Without these assessments, organisations struggle to prioritise security investments effectively or identify emerging vulnerabilities before they can be exploited (Sukumar et al., 2023).

Figure 16: Primary Responsibility for Cybersecurity Decisions



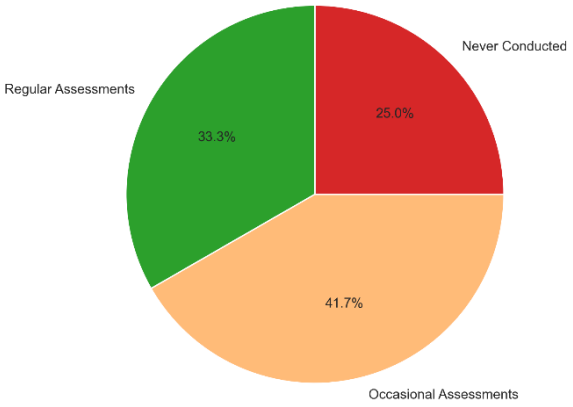
[16]

Source: Author's survey data (N=106), 2025

[15] Figure 15 demonstrates the positive correlation between training programmes and perceived effectiveness. Organisations with formal training report substantially higher effectiveness ratings for both communication and governance compared to those without training.

[16] Figure 16 shows that cybersecurity decisions are predominantly made by IT departments (50 %) or general management (33.3%). Limited involvement from dedicated cybersecurity personnel suggests a potential expertise gap, as those making security decisions may lack specialised security knowledge.

Figure 17: Frequency of Risk Assessment Conduct



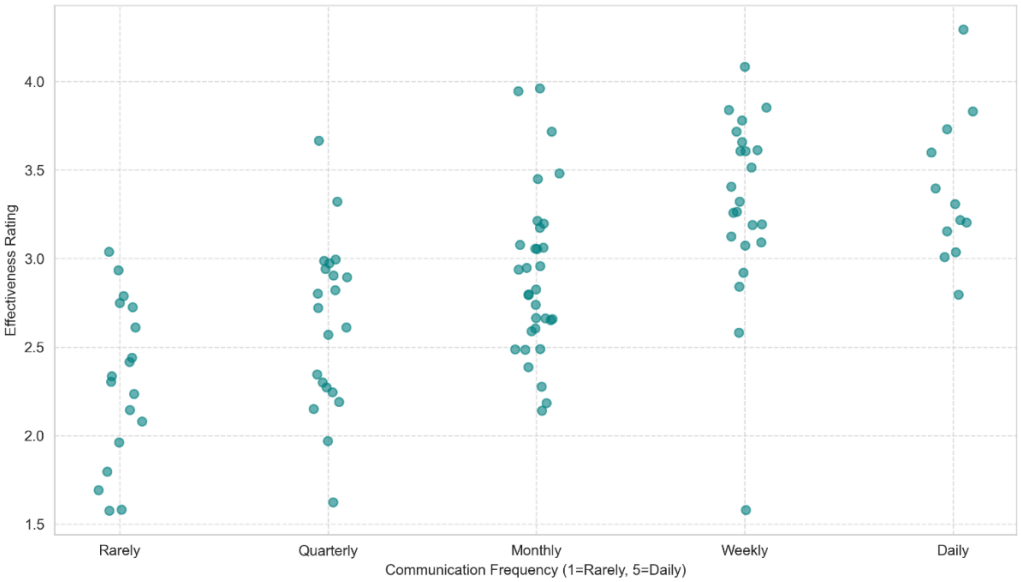
[17]

Source: Author's survey data (N=106), 2025

5.6 Relationships Between Variables

Governance effectiveness was seen to be generally higher when risk assessments were conducted more frequently, underscoring the importance of assessment as a foundation for effective governance (Haastrecht et al., 2021). Communication effectiveness was also higher with more frequent communication, but the relationship was not strictly linear. This suggests that while regular communication is important, the quality and relevance of the information shared are equally crucial for it to be effective (Corradini, 2020).

Figure 18: Communication Frequency vs. Effectiveness Scatter Plot



[18]

Source: Author's survey data (N=106), 2025

[17] Figure 17 reveals that only one-third of SMEs conduct regular risk assessments. The majority either assess occasionally or never, meaning most organisations lack a clear understanding of their cybersecurity risk profile and cannot effectively prioritise security investments.

[18] Figure 18 illustrates the relationship between communication frequency and perceived effectiveness. While effectiveness generally increases with frequency, the relationship is not strictly linear, indicating that the quality and relevance of communication matter as much as how often it occurs.

Notably, there appeared to be no significant correlation between the age of an organisation and any of the cybersecurity practices examined. This suggests that the maturity of cybersecurity practices is not necessarily tied to how long an SME has been in business, as younger organisations sometimes demonstrate better security habits than more established ones. Similarly, there appears to be no significant link between a business's annual revenue and the quality of its cybersecurity measures.

This implies that an SME's financial capacity does not automatically translate into better protection. Instead, factors such as organisational culture, leadership commitment, and industry-specific risks seem to play far more significant roles in determining how well a business manages its cyber threats (Onumo et al., 2021).

Figure 19: Correlation Matrix Heatmap

[19]

Source: Author's analysis, 2025

[19] Figure 19 presents a correlation matrix heatmap showing relationships between key variables. Notably, there is no significant correlation between organisational age or revenue and cybersecurity practices, suggesting that factors such as organisational culture, leadership commitment, and industry-specific risks play more significant roles than size or age alone.

6.0 Recommendations for SMEs

6.1 Implementation Philosophy

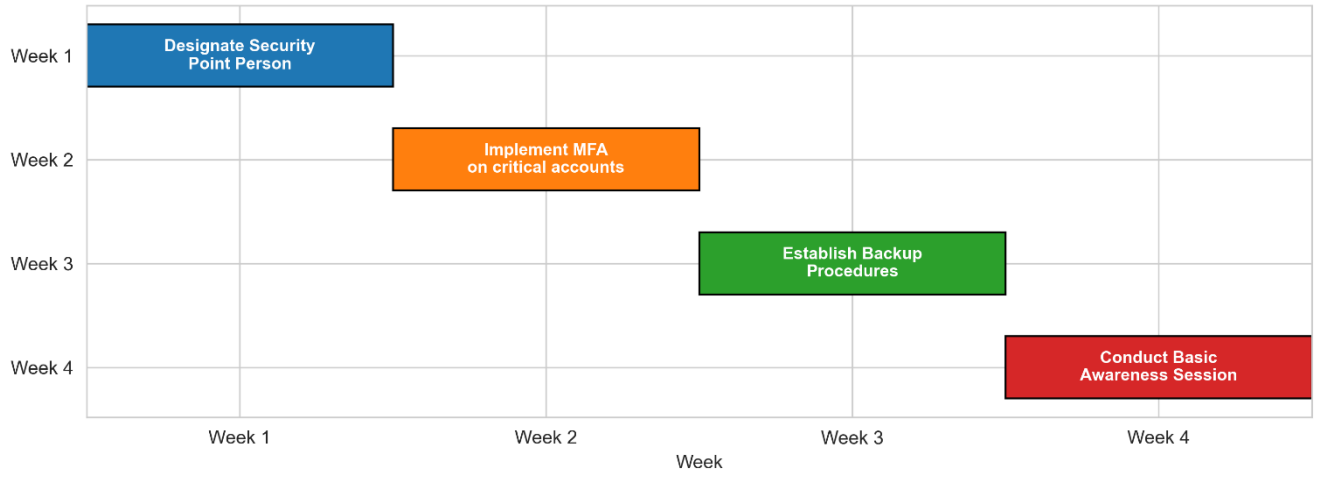
Every SME operates at a different maturity level, each with unique resources, risk profiles, and business requirements (Shojaifar & Järvinen, 2021). The recommendations that follow are organised by implementation timeline, allowing businesses to start with immediate, low-cost actions appropriate to their current state and progressively build capability over time. The goal is progress, not perfection; organisations that implement basic controls consistently will be far more secure than those that attempt ambitious programmes they cannot sustain.

6.2 Immediate Actions

In the first thirty days, SMEs should focus on foundational steps that require minimal investment but offer significant risk reduction. One of the most important actions is assigning cybersecurity responsibility to a specific individual who will be the security point person, even if it is a part-time role added to existing duties (Neri et al., 2023). This will become the primary contact for security decisions, incident response coordination, and communication with external resources. Establishing clear ownership is a crucial first step towards accountability.

Multi-factor authentication (MFA) should be implemented on all critical accounts, including email, banking, cloud services, and administrative access to business systems (CISA, 2023). MFA prevents the majority of credential-based attacks, even when passwords are compromised. Free tools like Google Authenticator make this protection accessible to SMEs regardless of their budget. Additionally, backup procedures must be established immediately. This involves creating regular, automated backups of all critical business data, stored separately from primary systems - ideally in cloud storage or offline media (CISA, 2023). Testing these restoration procedures is essential to ensure backups work when needed. This single measure is one of the most effective defences against ransomware and data loss.

Figure 20: Immediate Actions Timeline (First 30 Days)



20

Source: CISA, 2023; NIST, 2018; Bada & Nurse, 2019

[20] Figure 20 provides a week-by-week timeline for implementing immediate actions in the first 30 days. Each foundational step requires minimal investment but delivers significant risk reduction.

Basic awareness sessions should be conducted with all staff to discuss the most common threats facing the business, such as phishing, password security, and mobile device safety (Bada & Nurse, 2019). These sessions provide an opportunity to establish clear, practical policies that everyone can follow. For instance, staff should be instructed never to share passwords, to always verify requests for money transfers by phone, and to seek guidance before clicking on any links in suspicious emails.

6.3 Short-Term Initiatives

In the 30 to 90 days that follow, SMEs should focus on developing core security policies that cover key areas such as password requirements, acceptable use of company devices, data handling procedures, mobile device security, and incident reporting protocols (NIST, 2018). These policies should be straightforward and written in plain language to ensure all employees can understand them. Once created, the policies must be shared with everyone in the organisation.

Before investing in costly security solutions, businesses should make the most of security features already available. Activating tools like Microsoft Defender, using free antivirus software, implementing free password managers, and enabling automatic security updates for all software can offer significant protection without extra expense (Shojaifar & Fricker, 2023).

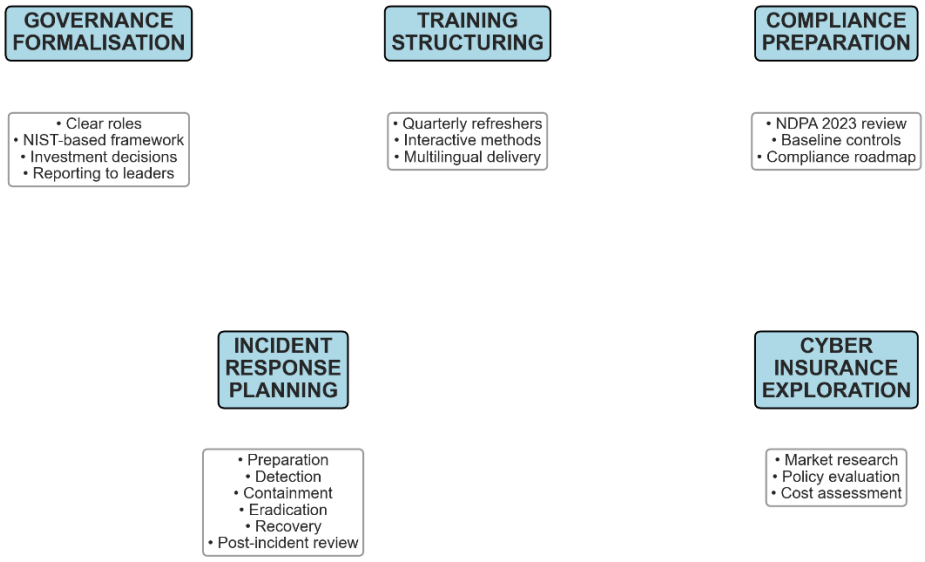
To identify security gaps and prioritise improvements, SMEs can use free, simplified self-assessment tools. For example, the UK's Cyber Essentials scheme provides an accessible checklist that Nigerian SMEs can adapt to their own context, offering a clear and structured way to evaluate current security practices (NCSC, 2023).

6.4 Medium-Term Building

In the 3 to 12 month timeframe, organisations should formalise their governance structures by clearly defining roles and responsibilities for security. They should establish simplified governance frameworks based on the principles of the NIST-CSF, create formal decision-making processes for security investments, and implement regular reporting on the organisation's security posture to leadership (Antunes et al., 2022).

During this period, training programmes should also evolve beyond one-off awareness sessions to recurring sessions. This includes conducting quarterly refresher training using interactive methods and delivering content in multiple languages to suit the workforce (Taherdoost, 2024). Training should be relevant to employees' actual work contexts and focus on practical exercises that build skills, rather than simply providing information.

Figure 21: Medium-Term Building Blocks (3-12 Months)



[21]

Source: Adapted from NIST, 2018; Ikuero & Zeng, 2022; Adriko & Nurse, 2024

Regulatory compliance should be addressed by reviewing obligations under the Nigeria Data Protection Act 2023 and implementing baseline controls to meet these requirements (Ardo et al., 2023). While achieving full compliance may take time, understanding the legal obligations and beginning to put controls in place shows a clear commitment to data protection.

Incident response plans should be developed to cover all key stages: preparation, detection, containment, eradication, recovery, and post-incident review (Ikuero & Zeng, 2022). Having a documented plan ensures that responses to incidents are coordinated and effective, rather than improvised under pressure. Cyber insurance options available in the Nigerian market should also be investigated. While insurance does not prevent attacks, it can provide critical financial support for recovery when prevention fails (Adriko & Nurse, 2024).

6.5 Long-Term Maturity

After the first year, organisations should focus on building a culture of continuous improvement. This involves conducting annual comprehensive security assessments, performing regular vulnerability scans and penetration tests, and systematically reviewing and updating policies and procedures. Staying informed about emerging threats and participating in industry threat intelligence sharing are also important to maintain strong security practices (Carias et al., 2020).

As organisations mature, they may adopt advanced security capabilities tailored to their needs. These can include security information and event management (SIEM) systems, professional threat intelligence services, regular penetration testing by qualified experts, and advanced employee testing such as social engineering assessments (Saeed et al., 2023). Pursuing certifications should also be considered when and where appropriate. This might include ISO 27001 for internationally

[21] Figure 21 illustrates the five key building blocks for medium-term cybersecurity development. Each block represents a critical area that SMEs should address within the 3-to-12-month timeframe.

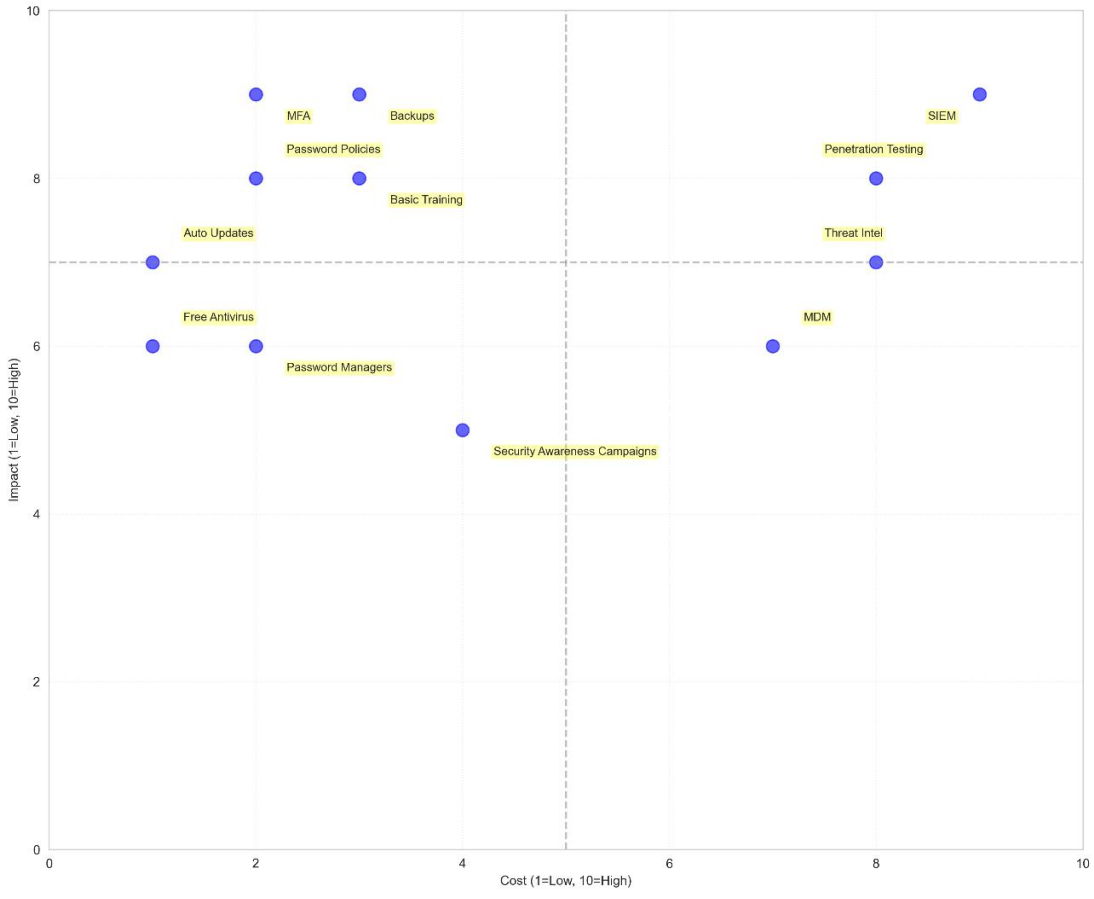
recognised information security management, sector-specific certifications like PCI DSS for payment processing, and the Nigerian national cybersecurity baseline certification once it becomes available (Alfaadhel et al., 2023).

The final stage of maturity is industry leadership. At this level, organisations share lessons learned to support other SMEs, mentor less mature businesses within their supply chains, contribute to the development of industry standards, and advocate for cybersecurity policies that support SMEs.

6.6 Cost-Effective Security

Research consistently shows that basic security hygiene can prevent majority of successful cyberattacks (CISA, 2023). Nigerian SMEs can significantly reduce their risk with minimal investment by focusing on free or low-cost technical controls such as multi-factor authentication, regular backups, and built-in security features. Alongside these, behavioural and organisational measures like staff training, clear policies, and defined accountability are essential. SMEs should also make the most of existing tools and platforms instead of [unnecessarily] purchasing new solutions. Collaborative approaches, including shared security services and industry partnerships, can further strengthen their defences (Shojaifar & Fricker, 2023). Ultimately, The most expensive security breach is the one that could have been prevented by basic measures..

Figure 22: Cost-Effective Security Prioritisation Matrix



[22]

Source: Author's analysis based on CISA, 2023; Shojaifar & Fricker, 2023

[22] Figure 22 presents a prioritisation matrix for cost-effective security investments. Measures in the upper-left quadrant (MFA, backups, basic training, password policies) deliver the highest impact at the lowest cost and should be prioritised by all SMEs regardless of budget constraints.

7.0 Policy Recommendations

7.1 The Case for Government Intervention

While SMEs must take ownership of their security posture, certain market forces present significant challenges to solving the cybersecurity crisis facing Nigeria's SME sector (Ardo et al., 2023). The resource limitations, knowledge gaps, and systemic issues common in this sector require strategic government intervention to create an environment where SMEs can operate securely and grow. Without such support, the gap between the level of cyber threats and the capabilities of SMEs will continue to widen, posing risks not only to individual businesses but also to the wider economy (Ibrahim et al., 2024).

7.2 Dedicated SME Cybersecurity Support Infrastructure

The creation of a dedicated SME Cybersecurity Support Office within an existing agency such as SMEDAN, NITDA, or NDPC would provide a central resource hub serving as a single point of contact for SMEs seeking guidance, tools, and support (Oyedeji et al., 2024). This office would coordinate cybersecurity initiatives across government agencies, private sector organisations, and international partners, ensuring that efforts are aligned rather than fragmented. It would maintain a knowledge repository of SME-appropriate tools, templates, policies, and case studies, making it easier for businesses to find and implement proven solutions. In addition, a help desk would provide direct assistance to SMEs facing cyber incidents or seeking implementation guidance, providing practical support when it is needed.

The development and distribution of a comprehensive National SME Cybersecurity Toolkit would provide SMEs with simplified risk assessment templates, policy and procedure templates for acceptable use, incident response, and data protection, as well as training materials in multiple Nigerian languages. The toolkit would also include step-by-step guides for implementing foundational controls, directories of vetted affordable security service providers, and incident response playbooks (NCSC, 2023).

7.3 National SME Cybersecurity Framework

Building on NITDA's existing cybersecurity initiatives, a Nigeria Cyber Essentials Framework should be created as a simplified, practical, technical baseline adapted to Nigerian SME contexts (NITDA, 2023). To be effective, this framework must be accessible, providing plain-language guidance that avoids the technical-speak that often alienates non-specialist readers. It should also be affordable, with a strong emphasis on low-cost and no-cost controls that businesses can implement regardless of their budget constraints.

A tiered approach, offering levels such as Bronze, Silver, and Gold, would allow organisations to demonstrate progressive maturity over time. The framework should be certifiable, and must be adaptable, offering sector-specific guidance for high-risk industries such as finance, healthcare, and education.

The table below, adapted from NCSC (2023) and NITDA (2023), outlines these five core characteristics. Each one is designed to address a specific barrier that currently prevents Nigerian SMEs from adopting international cybersecurity standards.

Table 2: Characteristics of the Proposed Nigeria Cyber Essentials Framework

Proposed Characteristics	Description
Accessible	Plain-language guidance that is easy to understand
Affordable	A focus on low-cost and no-cost security controls
Tiered	Progressive levels (e.g., Bronze, Silver, Gold) to track maturity.
Certifiable	Options for self-assessment and third-party verification
Adaptable	Sector-specific guidance for high-risk industries

7.4 Strengthen and Clarify Regulatory Framework

The Nigeria Data Protection Commission should consider publishing a comprehensive SME Compliance Handbook for the Nigeria Data Protection Act 2023, providing clear and actionable guidance tailored specifically to small business contexts (NDPC, 2023). This handbook would translate complex regulatory requirements into practical steps that SMEs can easily understand and implement. A proportionate, tiered compliance framework should be developed alongside this handbook that recognises the diversity within the sector, scaling requirements to match an organisation's actual capacity and risk exposure (Ardo et al., 2023). Under this model, micro-enterprises would not face the same compliance burden as medium-sized firms, ensuring that regulations are calibrated to reflect real-world risk levels.

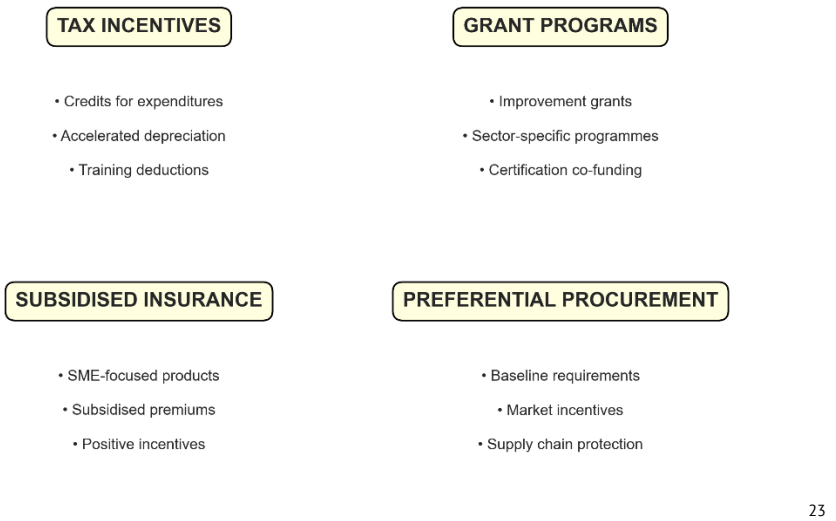
In implementing this, a *support-first* enforcement approach should be adopted that incorporates grace periods that prioritise education and assistance over immediate penalties (Ikuero & Zeng, 2022). This strategy acknowledges that while many SMEs intend to comply, they often lack the necessary knowledge and resources. Punitive measures against well-intentioned but under-resourced businesses can be counterproductive, potentially stifling growth without improving security.

Punitive enforcement should instead be reserved for cases of wilful negligence, repeat violations, or incidents that cause significant harm. By focusing on guidance first, the regulatory environment can encourage continuous improvement and help businesses close initial gaps, while still maintaining accountability for serious or deliberate failures.

7.5 Create Economic Incentives

Tax incentives such as credits for qualifying cybersecurity expenses, accelerated depreciation on cybersecurity infrastructure investments, and enhanced deductions for employee cybersecurity training and certification would help make security investments more affordable for cash-constrained SMEs (PwC, 2023). Grant and subsidy programmes could support SMEs by offering cybersecurity improvement grants with matched funding models, sector-specific initiatives targeting high-priority industries, and government co-funding to cover costs associated with ISO 27001 or national baseline certification. These measures would directly address the resource limitations that often prevent SMEs from implementing adequate security measures (World Bank, 2022).

Figure 23: Economic Incentives for Cybersecurity Investment



[23]

Source: PwC, 2023; World Bank, 2022; Adriko & Nurse, 2024

Subsidised cyber insurance products designed specifically for SMEs, developed through partnerships with the insurance industry, could also lower premiums for businesses that meet national baseline security requirements, with positive incentives for security investment helping create market mechanisms that reward good cybersecurity practices (Adriko & Nurse, 2024). Preferential government procurement policies requiring contractors to comply with the national cybersecurity baseline would further encourage certification uptake while simultaneously protecting government systems from supply chain risks.

7.6 Build National Cybersecurity Capacity

Education integration should include cybersecurity awareness in primary and secondary school curricula, the establishment of *general studies* tracks for cybersecurity in polytechnics and universities, and support for faculty development and research capacity (NITDA, 2023). Building awareness and skills at all educational levels helps create a pipeline of future talent while raising general cybersecurity literacy across the population.

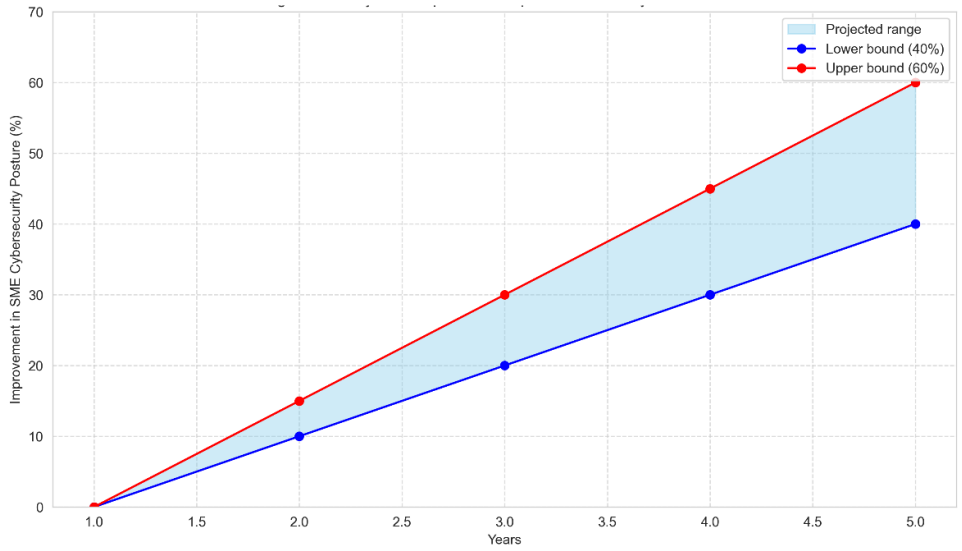
A national cybersecurity training centre offering affordable professional certifications alongside specialised training for SME security practitioners and train-the-trainer programmes would amplify the impact of training investments by continuously developing local capacity to provide ongoing education (ISC2, 2023). Scholarship and retention programmes that offer cybersecurity scholarships tied to service commitments in Nigeria, support for internationally recognised certifications, and competitive public sector career paths would help retain skilled professionals who might otherwise seek opportunities abroad.

[23] Figure 23 presents a comprehensive framework of economic incentives across four categories: tax incentives, grant programmes, subsidised insurance, and preferential procurement. Together, these mechanisms create multiple pathways for making cybersecurity investment more accessible and attractive to SMEs.

7.7 Policy Impact Potential

Research from comparable contexts suggests that comprehensive policy interventions - combining regulation, economic incentives, capacity building, and public-private collaboration - can contribute about a 40 to 60% improvement in SME cybersecurity posture within 3 to 5 years (ENISA, 2021). For Nigeria, this improvement could make the difference with thousands of businesses better protected, billions of naira in avoided losses, and overall, stronger national economic security. The investment needed to achieve these outcomes is modest when compared to the economic costs of ongoing vulnerabilities and escalating losses.

Figure 24: Projected Impact of Comprehensive Policy Interventions



[24]

Source: ENISA, 2021; Author's projections

[24] Figure 24 projects the potential impact of comprehensive policy interventions combining regulation, economic incentives, capacity building, and public-private collaboration. Research from comparable contexts suggests that such integrated approaches can achieve up to 40 to 60% improvement in SME cybersecurity posture within 3 to 5 years.

8.0 Conclusion

There is a pressing need for Nigerian SMEs to enhance their cybersecurity risk communication and governance practices. The lack of formal training programmes, infrequent communication, and limited cybersecurity expertise documented in this research contribute directly to the heightened vulnerability that characterises the SME sector (Pereye et al., 2025; Benjamin et al., 2024). Addressing these challenges requires a proactive approach that prioritises regular risk assessments, diverse communication strategies, tailored training programmes, and the establishment of robust cybersecurity governance structures. By adopting the phased framework and implementing the recommendations outlined in this Report, Nigerian SMEs can cultivate a proactive cybersecurity culture that empowers employees at all levels to identify and mitigate risks effectively (Corradini, 2020; Carias et al., 2020). The path forward is clear, but it requires commitment from business owners, support from government, and collaboration across the entire business community.

Securing Nigeria's SME sector is not merely a business imperative but a matter of economic and national security (Ibrahim et al., 2024). A collaborative, multi-stakeholder approach can transform Nigeria's cybersecurity posture from a position of vulnerability into a competitive advantage in the global digital economy. This vision is achievable. It requires commitment, investment, and sustained effort from all stakeholders. The alternative, continued vulnerability and escalating losses, is far more costly.

References

Abdul-Azeez, O., Ihechere, A. O., & Idemudia, C. (2024). Digital access and inclusion for SMEs in the financial services industry through Cybersecurity GRC. *Finance & Accounting Research Journal*, 6(7), 1134-1156.

Adriko, R., & Nurse, J. R. C. (2024). Cybersecurity, cyber insurance and small-to-medium-sized enterprises: A systematic Review. *Information & Computer Security*.

Akpan, I. J., Udoh, E. E., & Adebisi, B. (2020). Small business awareness and adoption of state-of-the-art technologies in emerging and developing markets. *Journal of Small Business & Entrepreneurship*, 34(2), 123-140.

Alfaadhel, A., Almomani, I., & Ahmed, M. (2023). Risk-Based Cybersecurity Compliance Assessment System (RC2AS). *Applied Sciences*, 13(10), 6145.

Antunes, M., Maximiano, M., & Gomes, R. (2022). A Client-Centered Information Security and Cybersecurity Auditing Framework. *Applied Sciences*, 12(9), 4102.

Ardo, A. A., Bass, J. M., & Gaber, T. (2023). Implications of regulatory policy for building secure agile software in Nigeria: A grounded theory. *The Electronic Journal of Information Systems in Developing Countries*, 89(6), e12285.

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information & Computer Security*, 27(3), 393-410.

Benjamin, L. B., Adegbola, A. E., Amajuoyi, P., Adegbola, M. D., & Adeusi, K. B. (2024). Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies. *Global Journal of Engineering and Technology Advances*, 19(2), 134-153.

Carias, J. F., Borges, M. R. S., Labaka, L., Arrizabalaga, S., & Hernantes, J. (2020). Systematic Approach to Cyber Resilience Operationalization in SMEs. *IEEE Access*, 8, 174200-174221.

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2023). A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises. *Computer Science Review*, 50, 100592.

CISA. (2023). *Cyber Essentials Toolkit*. Cybersecurity and Infrastructure Security Agency.

Corradini, I. (2020). Building a cybersecurity culture. In I. Corradini, *Building a Cybersecurity Culture in Organizations* (pp. 63-86). Springer.

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance*, 47(3), 698-736.

CYFIRMA. (2025). Dark web monitoring report: Nigerian data exposure. CYFIRMA Research.

Deloitte. (2025). Financial services cybersecurity outlook: Africa region. Deloitte Insights.

ENISA. (2021). *Cybersecurity for SMEs: Challenges and recommendations*. European Union Agency for Cybersecurity.

Ewuga, S. K., Egieya, Z. E., Omotosho, A., & Adegbite, A. O. (2023). Comparative review of technology integration in SMEs: A tale of two economies. *Engineering Science & Technology Journal*, 4(6), 555-570.

Falowo, O. I., Popoola, S., Riep, J., Adewopo, V. A., & Koch, J. (2022). Threat actors' tenacity to disrupt: Examination of major cybersecurity incidents. *IEEE Access*, 10, 134038-134051.

Foli, S., Durst, S., Davies, L., & Temel, S. (2022). Supply Chain Risk Management in Young and Mature SMEs. *Journal of Risk and Financial Management*, 15(8), 328.

Guardian Nigeria. (2022, July 11). Cyber attack on Nigerian SMEs up by 89 % in 2022. *The Guardian*.

Haastrecht, M., Sarhan, I., Shojaifar, A., Baumgartner, L., Mallouli, W., & Spruit, M. (2021). A threat-based cybersecurity risk assessment approach addressing SME needs. *Proceedings of the 16th International Conference on Availability, Reliability and Security*, 1-12.

Ibrahim, Y. A., Ishaya, A. O., Yusuf, M., Nancy, I., Bijik, H. A., & Aiyedogbon, S. F. (2024). Cybersecurity and Cybercrimes in Nigeria: An Overview of Challenges and Prospects. *2024 International Conference on Science, Engineering and Business*, 1-7.

Iguodala-Cole, H. I. (2024). Navigating Cultural Norms and Sustainable Development in the Nigerian Workplace. *The Nigerian Journal of Sociology and Anthropology*, 22(1), 52-74.

Ikuero, F. E., & Zeng, W. (2022). Improving cybersecurity incidents reporting in Nigeria: Micro and small enterprises perspectives. *Nigerian Journal of Technology*, 41(3), 512-520.

ISC2. (2023). *Cybersecurity workforce study*. International Information System Security Certification Consortium.
ISO/IEC. (2022). *ISO/IEC 27001:2022 Information security management systems*. International Organization for Standardization.

Junior, C. R., Becker, I., & Johnson, S. (2023). Unaware, unfunded and uneducated: A systematic review of SME cybersecurity. *arXiv preprint*.

Kandpal, S., Bhatt, S., Mohan, L., Patwal, A., & Kumar, P. (2023). Cyber Security Implementation Issues in Small to Medium-sized Enterprises. *2023 14th International Conference on Computing Communication and Networking Technologies*, 1-5.

Khan, M. H., & Muntaha, S. T. (2024). Evaluating the effectiveness of cybersecurity awareness programs in reducing phishing attacks. *World Journal of Advanced Research and Reviews*, 23(2), 1663-1673.

Kori-Siakpere, U., Gokeme, O., Omale, R. O., Aniah, A. R., Ojukwu, P. M., & Okache, M. O. (2024). The Impact of Linguistic Diversity on Intercultural Communication in Nigerian Organizations. *Journal of Innovative Research*, 2(2), 25-33.

Lazarus, S., & Button, M. (2022). Tweets and reactions: Revealing the geographies of cybercrime perpetrators and the North-South divide. *Cyberpsychology, Behavior, and Social Networking*, 25(8), 504-511.

Melaku, H. M. (2023). A Dynamic and Adaptive Cybersecurity Governance Framework. *Journal of Cybersecurity and Privacy*, 3(3), 327-350.

Musabayana, G. T., Mutambara, E., & Ngwenya, T. (2023). Establishment of a Zimbabwe National SME sector. *Journal of Innovation and Entrepreneurship*, 12(1), 65.

Nadella, G. S., Gonaygunta, H., Kumar, D., & Pawar, P. P. (2024). Exploring the impact of AI-driven solutions on cybersecurity adoption in small and medium enterprises. *World Journal of Advanced Research and Reviews*, 22(1), 1199-1197.

Nairametrics. (2023, July 12). SMEs in Nigeria were major victims of cyber-attacks in 2022. *Nairametrics*.

NCC. (2023). *Subscriber statistics report*. Nigerian Communications Commission.

NCSC. (2023). Cyber Essentials: Requirements for IT infrastructure. National Cyber Security Centre.

NDPC. (2023). Nigeria Data Protection Act 2023: Implementation guidance. Nigeria Data Protection Commission.

Neri, M., Niccolini, F., & Martino, L. (2024). Organizational cybersecurity readiness in the ICT sector. *Information & Computer Security*, 32(1), 38-52.

NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. National Institute of Standards and Technology.

NITDA. (2023). *National Cybersecurity Policy and Strategy*. National Information Technology Development Agency.

Ogbeide, V. O., Omorogiuwa, O., & Salami, E. E. (2023). An empirical survey to substantiate the need for a cyber security framework for SMEs in Nigeria. *International Journal of Research Publications*, 128(1).

Ogunjimi, O., Afoloeunsho, A. A., & Olukomoro, O. (2018). Elicitation of SME Requirements for Cybersecurity Solutions. *Advances in Multidisciplinary & Scientific Research Journal*, 6(2), 29-34.

Okundaye, K., Fan, S. K., & Dwyer, R. J. (2019). Impact of information and communication technology in Nigerian small-to medium-sized enterprises. *Journal of Economics, Finance and Administrative Science*, 24(47), 29-46.

Oluokun, A., Idemudia, C., & Iyelolu, T. V. (2024). Enhancing digital access and inclusion for SMEs through Cybersecurity GRC. *Computer Science & IT Research Journal*, 5(7), 1576-1604.

Onumo, A., Ullah-Awan, I., & Cullen, A. (2021). Assessing the Moderating Effect of Security Technologies on Employees Compliance. *ACM Transactions on Management Information Systems*, 12(2), 1-29.

Oyedeji, O. C., Moronkunbi, M. A., Victor, A. A., & Victor, P. O. (2024). Assessing the Efficiency of Contemporary Cybersecurity Protocols in Nigeria. *International Journal of Latest Technology in Engineering Management & Applied Science*, 13(7), 52-58.

Özkan, B. Y., & Spruit, M. (2020). Cybersecurity Standardisation for SMEs: The Stakeholders' Perspectives. In *Research Anthology on Artificial Intelligence Applications in Security* (pp. 1252-1278). IGI Global.

Pereye, A., et al. (2025). Cybersecurity awareness and practices among small and medium-sized enterprises (SMEs) in Edo State, Nigeria. *International Journal of Scientific Research and Analysis*, 2(4), 81-95.

Perozzo, H., Zaghloul, F., & Ravarini, A. (2022). CyberSecurity Readiness: A Model for SMEs based on the Socio-Technical Perspective. *Complex Systems Informatics and Modeling Quarterly*, 33, 53-66.

Profiled Nigeria. (2025). *Q1 2025 Cybersecurity Threat Report*. Profiled Nigeria Research.

PwC. (2023). *Global Digital Trust Insights Survey*. PricewaterhouseCoopers.

Reis, O., Oliha, J. S., Osasona, F., & Obi, O. C. (2024). Cybersecurity dynamics in Nigerian banking: Trends and strategies review. *Computer Science & IT Research Journal*, 5(2), 336-364.

Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A Systematic Literature Review on Cyber Threat Intelligence. *Sensors*, 23(16), 7273.

Serianu. (2023). *Africa Cybersecurity Report*. Serianu Limited.

Shojaifar, A., & Fricker, S. A. (2023). Design and evaluation of a self-paced cybersecurity tool. *Information & Computer Security*, 31(2), 244-262.

Shojaifar, A., & Järvinen, H. (2021). Classifying SMEs for Approaching Cybersecurity Competence and Awareness. *Proceedings of the 16th International Conference on Availability, Reliability and Security*, 1-7.

SMEDAN. (2022). *National Survey of Micro, Small and Medium Enterprises*. Small and Medium Enterprises Development Agency of Nigeria.

Sukumar, A., Mahdiraji, H. A., & Jafari-Sadeghi, V. (2023). Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach. *Risk Analysis*, 43(10), 2082-2098.

Sutton, A., & Tompson, L. (2023). Towards a Cybersecurity Culture-Behaviour Framework: A Rapid Evidence Review.

Taherdoost, H. (2024). Towards an Innovative Model for Cybersecurity Awareness Training. *Information*, 15(9), 512.

VPN Alert. (2026). Ransomware statistics and trends for Nigeria. *VPN Alert Research*.

World Bank. (2022). Digital Development Partnership Annual Report. World Bank Group.

About the Author

Terdoofan Agber is a Digital Policy and Cyber Resilience professional dedicated to securing Africa's digital future. With experience spanning mission-critical support for the Nigerian Air Force to engineering global intelligence systems at GASA and Gogolook, she is a leading voice for socio-cognitive security. She argues that effective cyber policies must root themselves in local contexts, languages and indigenous knowledge, rather than remaining abstract technical requirements. A rising figure in Nigeria's digital diplomacy, she works at the intersection of anti-scam intelligence and data governance, ensuring global standards are harmonised with African socio-technical realities.

Website: https://tsokura.co/research/reports

Citation

Agber, T. (2026). Cyber Risk Management Insights for Nigerian SMEs: Practical Strategies for Risk Communication and Governance. Tsokura Research.

Published: March 2026