Magna Scientia Advanced Research and Reviews

eISSN: 2582-9394

Cross Ref DOI: 10.30574/msarr

Journal homepage: https://magnascientiapub.com/journals/msarr/

(REVIEW ARTICLE)

Check for updates

Cybersecurity Readiness in Developing Countries' Enterprises: A Comparative Multi-Case Analysis

Osita Victor Egwuatu *

MBA (Information Systems), College of Business and Innovation, The University of Toledo, Toledo, Ohio United States.

Magna Scientia Advanced Research and Reviews, 2025, 15(01), 068-083

Publication history: Received on 10 August 2025; revised on 14 September 2025; accepted on 18 September 2025

Article DOI: https://doi.org/10.30574/msarr.2025.15.1.0110

Abstract

The rapid digitalization of developing economies has expanded opportunities for innovation, financial inclusion, and enterprise growth, but it has also introduced significant cybersecurity risks. This study examines the cybersecurity readiness of small and medium-sized enterprises (SMEs) in Africa, with a focus on Nigeria, Kenya, and South Africa. Using a qualitative multi-case analysis supplemented by policy reports, secondary data, and cybersecurity indices, the study identifies key risks, phishing, ransomware, insider threats, and cloud vulnerabilities and evaluates enterprise practices against global standards such as the NIST Cybersecurity Framework (CSF) and ISO/IEC 27001. Findings indicate that most SMEs adopt ad-hoc tools, provide limited staff training, and lack formal incident response mechanisms, resulting in readiness levels far below international benchmarks. Comparative insights from India's Unified Payments Interface (UPI) and Brazil's PIX highlight the importance of institutional coordination and embedded regulatory oversight in enhancing resilience. The study contributes to Information Systems (IS) risk management and Resource-Based View (RBV) theory by framing cybersecurity readiness as a strategic capability that can enable competitive advantage. Policy implications emphasize digital literacy, workforce development, and regulatory harmonization, while practical recommendations encourage SMEs to integrate cybersecurity into business strategy as an enabler rather than a cost.

Keywords: Cybersecurity Readiness; Small and Medium-Sized Enterprises (SMEs); Developing Countries; NIST Cybersecurity Framework (CSF); ISO/IEC 27001; Digital Transformation

1. Introduction

1.1. Background: Rise of Digitalization in Africa and Other Developing Regions

Over the past two decades, Africa and other developing regions have undergone a rapid transformation driven by the proliferation of digital technologies. Internet penetration across the continent has expanded exponentially, supported by mobile connectivity, fintech innovations, and e-commerce platforms. According to the International Telecommunication Union (ITU), Africa's internet usage grew from less than 5% of the population in 2001 to over 43% in 2023, with mobile devices serving as the primary access point (ITU, 2023). This digital shift has enabled enterprises of all sizes, particularly small and medium-sized enterprises (SMEs), to engage in cross-border trade, improve service delivery, and tap into global markets.

Digitalization has been particularly prominent in sectors such as mobile banking, logistics, health technology, and e-commerce. Platforms such as M-Pesa in Kenya, Flutterwave and Paystack in Nigeria, and Jumia in pan-African markets demonstrate how businesses in resource-constrained environments are leapfrogging traditional infrastructures to

* Corresponding author: Osita Victor Egwuatu

adopt innovative, technology-driven solutions (Aker & Mbiti, 2019). Beyond Africa, similar patterns are evident in South Asia and Latin America, where digital ecosystems are reshaping enterprise operations and national economies.

While digitalization has provided opportunities for economic growth, financial inclusion, and social development, it has also introduced new vulnerabilities. The increased reliance on technology means that enterprises are exposed to cyber risks that threaten their operational continuity, customer trust, and financial stability. Unlike in developed economies, where robust cybersecurity frameworks and investments are commonplace, enterprises in developing regions often operate in fragile environments characterized by inadequate regulatory oversight, limited financial resources, and scarce cybersecurity expertise.

1.2. Cybersecurity as Both a Global and Local Challenge

Cybersecurity has emerged as one of the most pressing global challenges of the 21st century. Worldwide, cybercrime is projected to cost the global economy over $10.5 trillion annually by 2025, making it more profitable than the trade in all major illegal drugs combined (Cybersecurity Ventures, 2021). The growing sophistication of cyber threats, including ransomware, phishing, distributed denial-of-service (DDoS) attacks, and insider threats, demands proactive defense mechanisms that align with international best practices.

At the global level, frameworks such as the **NIST Cybersecurity Framework (CSF)**, **ISO/IEC 27001**, and the **European Union's General Data Protection Regulation (GDPR)** have established benchmarks for cyber readiness. These frameworks emphasize risk management, governance, continuous monitoring, and regulatory compliance as pillars of enterprise resilience. However, the implementation of such frameworks in developing regions remains limited, owing to contextual differences.

At the local level, African enterprises face unique cybersecurity challenges shaped by their socio-economic and infrastructural realities. For example, widespread use of mobile banking and digital wallets has increased vulnerabilities to fraud, SIM-swapping, and account takeovers. SMEs, which make up over 80% of employment in Africa (World Bank, 2020), often lack the financial and technical capacity to implement advanced cybersecurity controls. Moreover, weak enforcement of data protection regulations, limited cross-border cooperation, and a shortage of skilled cybersecurity professionals exacerbate the risks.

Thus, cybersecurity readiness is simultaneously a **global concern** requiring alignment with international standards and a **local challenge** shaped by contextual realities. Addressing both dimensions is critical to ensuring that African enterprises can harness the benefits of digitalization without succumbing to crippling cyber incidents.

1.3. Research Problem: Enterprises Lack Adequate Frameworks to Manage Cyber Risk

Despite the rapid digital adoption, the cybersecurity readiness of African enterprises remains alarmingly low. A 2022 report by Deloitte revealed that fewer than 30% of surveyed African organizations had a formalized cybersecurity strategy, and over 60% relied on reactive approaches to cyber incidents rather than proactive defense mechanisms (Deloitte, 2022). Similarly, the ITU's Global Cybersecurity Index ranks several African countries in the lower tiers, reflecting gaps in regulatory enforcement, incident response infrastructure, and public-private cooperation.

The problem is compounded for SMEs, which form the backbone of developing economies but often operate informally and with limited resources. These enterprises are less likely to conduct formal risk assessments, maintain updated security patches, or invest in staff training. Many depend on outsourced IT services, which may not prioritize cybersecurity, thereby increasing their vulnerability to both internal and external threats. The reliance on cloud-based solutions and mobile platforms often without adequate encryption, authentication, or access controls further intensifies exposure.

In effect, the absence of structured, scalable, and context-sensitive cybersecurity frameworks undermines enterprise resilience, disrupts economic growth, and erodes trust in digital ecosystems. Without intervention, the progress made in digitalization risks being reversed by increasingly sophisticated cyber threats.

1.4. Research Objectives

This study aims to address the identified gaps by focusing on three interrelated objectives:

1.4.1. Analyze key cyber risks for African SMEs.

The first objective is to map the predominant cybersecurity risks facing enterprises in African markets. These risks include phishing attacks, ransomware, insider threats, supply chain vulnerabilities, and regulatory non-compliance.

1.4.2. Assess readiness frameworks compared to global standards.

The second objective is to evaluate existing cybersecurity practices within African enterprises against international benchmarks such as NIST CSF and ISO/IEC 27001. This comparative analysis will highlight the gaps and contextual constraints that limit adoption in resource-constrained settings.

1.4.3. Recommend scalable defense strategies.

The third objective is to propose practical, cost-effective defense strategies tailored to African enterprises. These strategies include cloud-based security services, capacity-building initiatives, public-private partnerships, and regional cybersecurity cooperation.

Together, these objectives seek to build a holistic understanding of how developing countries can strengthen enterprise cybersecurity readiness while aligning with global best practices.

1.5. Contribution: Filling the Research Gap in Developing-World Cybersecurity Literature

Existing research on cybersecurity readiness has largely been dominated by studies in North America, Europe, and parts of Asia, where regulatory regimes are more mature and enterprises have greater access to resources (Von Solms & Van Niekerk, 2013). In contrast, the experiences of developing countries, particularly in Africa, have been underrepresented in academic and policy-oriented literature. This creates a knowledge gap that undermines the ability of global stakeholders to design inclusive cybersecurity policies and frameworks.

By focusing on African enterprises, this study contributes in several significant ways:

- **Empirical Contribution:** It documents the current state of cyber readiness in African SMEs, an area with limited existing research.
- **Theoretical Contribution:** It integrates Information Systems (IS) risk management with global cybersecurity frameworks, thereby contextualizing theories of risk and resilience in developing-world settings.
- **Practical Contribution:** It provides policymakers, enterprise leaders, and international organizations with actionable strategies to strengthen cybersecurity resilience without imposing unsustainable costs.
- **Policy Contribution:** It underscores the need for international cooperation, regulatory harmonization, and capacity-building to ensure that Africa and other developing regions are not left behind in the global cybersecurity landscape.

1.6. Conclusion of the Introduction

The rise of digitalization in Africa has created immense opportunities for economic growth, innovation, and global integration. However, the corresponding rise in cyber risks poses existential threats to enterprises that lack adequate frameworks to manage these challenges. Cybersecurity is no longer a peripheral issue but a central concern for enterprise sustainability and competitiveness.

This study addresses the urgent need for research that bridges global cybersecurity standards with local realities in developing regions. By analyzing risks, assessing readiness frameworks, and recommending scalable defense strategies, it seeks to contribute to both academic scholarship and practical policymaking. In doing so, it aims to ensure that African enterprises can not only survive but thrive in an increasingly interconnected digital economy.

2. Literature Review

2.1. Global Perspective on Cybersecurity Frameworks

Cybersecurity has become a global priority, with governments, corporations, and international organizations recognizing the need for structured approaches to managing digital risks. Several frameworks dominate the global discourse, providing benchmarks for readiness and resilience.

One of the most influential is the **NIST Cybersecurity Framework (CSF)**, developed by the U.S. National Institute of Standards and Technology. It provides a risk-based, flexible structure consisting of five core functions: Identify, Protect, Detect, Respond, and Recover (NIST, 2018). The NIST CSF emphasizes continuous monitoring, layered defenses, and organizational governance, making it widely adopted across industries and increasingly referenced in international policy discussions.

Similarly, **ISO/IEC 27001** is a globally recognized standard for information security management systems (ISMS). It establishes systematic processes for managing sensitive information, including risk assessment, incident response, and compliance (ISO, 2017). Unlike the NIST CSF, which is more of a guiding framework, ISO/IEC 27001 requires formal certification, making it particularly appealing to multinational corporations and highly regulated industries such as finance and healthcare.

In addition to frameworks, **regulations** play a critical role in shaping enterprise cybersecurity. The **European Union's General Data Protection Regulation (GDPR)**, implemented in 2018, is one of the most far-reaching pieces of legislation, setting stringent requirements for data protection, breach notification, and consumer rights (Voigt & Von dem Bussche, 2017). GDPR has not only transformed practices within the EU but also influenced global compliance norms, with many African and Asian countries adopting GDPR-inspired laws.

Collectively, these frameworks and regulations underscore the importance of **structured, proactive, and compliance-driven approaches** to cybersecurity. Enterprises in developed economies typically align with at least one of these models, often investing heavily in technology, skilled personnel, and audits to ensure continuous readiness.

2.2. Cybersecurity in Developing Countries: Challenges and Realities

While global frameworks provide strong models, their implementation in developing countries has been inconsistent and fragmented. Several studies point to systemic challenges limiting adoption.

- **Regulatory Fragmentation:** Many developing countries lack comprehensive cybersecurity laws or effective enforcement mechanisms. For instance, while nations such as Nigeria, Kenya, and South Africa have enacted data protection regulations, others remain in early stages of drafting policies. Even where regulations exist, enforcement capacity is limited due to resource constraints, bureaucratic inefficiencies, and competing policy priorities (Oguya, 2021). This regulatory patchwork results in uneven standards across industries and regions.
- **Workforce Shortages:** A recurring challenge is the shortage of skilled cybersecurity professionals. The World Economic Forum (2022) estimates a global shortage of 3.4 million cybersecurity workers, with Africa bearing a disproportionate share of this gap. Enterprises often depend on general IT staff to handle cybersecurity tasks, which leads to insufficient expertise in risk assessment, incident detection, and compliance management. This lack of skilled labor undermines the adoption of sophisticated frameworks like ISO 27001 or NIST CSF.
- **Dependence on Foreign Vendors:** Many African enterprises rely on third-party vendors often multinational cloud providers, for digital infrastructure and security tools. While this reliance provides access to cutting-edge technologies, it also introduces vulnerabilities such as vendor lock-in, inadequate local support, and exposure to geopolitical risks (Mutimukwe & Kimeli, 2020). Moreover, small enterprises often lack the bargaining power to negotiate service-level agreements that adequately protect them from cyber incidents.
- **Cost and Resource Constraints:** Cybersecurity investments require significant financial resources, including expenditure on firewalls, intrusion detection systems, training programs, and audits. For SMEs operating in resource-constrained environments, these costs are prohibitive. As a result, enterprises often adopt reactive rather than proactive approaches, investing only after a major incident has occurred (PwC Africa, 2021).
- **Cultural and Awareness Barriers:** Cybersecurity readiness is also hindered by low levels of awareness among business leaders and employees. Many SMEs perceive cybersecurity as a purely technical issue rather than a strategic one, which leads to underinvestment in governance and staff training (Kshetri, 2019).

Together, these challenges illustrate the gap between global cybersecurity norms and local realities in developing countries, where enterprises often lack both the institutional and material capacity to implement robust frameworks.

2.3. Theoretical Lenses

To analyze cybersecurity readiness in African enterprises, three theoretical lenses are particularly useful: IS Risk Management, the Resource-Based View (RBV), and the Technology Acceptance Model (TAM).

2.3.1. IS Risk Management Frameworks

Information Systems (IS) risk management frameworks provide structured methodologies for identifying, assessing, and mitigating risks. Widely referenced frameworks such as COBIT, OCTAVE, and FAIR emphasize the role of governance, risk assessment, and control mechanisms (Von Solms & Van Niekerk, 2013). Applying IS risk management in developing countries highlights how enterprises evaluate threats, prioritize controls, and allocate resources in environments with severe financial and skills constraints. This lens helps contextualize why many SMEs default to ad-hoc approaches and what trade-offs they make in balancing cost and risk.

2.3.2. Resource-Based View (RBV)

RBV posits that competitive advantage arises from the strategic deployment of valuable, rare, inimitable, and non-substitutable resources (Barney, 1991). Cybersecurity readiness can be understood as an organizational capability that differentiates firms in competitive markets. For African SMEs, robust cybersecurity practices can become a source of trust and resilience, enabling access to international markets, partnerships, and investment. However, the scarcity of skilled personnel and financial resources constrains their ability to build these capabilities internally, leaving them vulnerable to cyber risks.

2.3.3. Technology Acceptance Model (TAM)

The Technology Acceptance Model explains the adoption of new technologies based on perceived usefulness and ease of use (Davis, 1989). Applied to cybersecurity, TAM helps explain why African enterprises may resist or adopt security tools. For instance, SMEs may avoid multi-factor authentication systems if perceived as too complex, even if they acknowledge their usefulness. Conversely, they may adopt cloud-based security services if they are perceived as easy to implement and maintain. TAM provides insights into behavioral factors influencing readiness beyond purely economic or regulatory considerations.

Together, these theoretical perspectives offer a multidimensional view: IS risk management frames the process, RBV frames the strategic value, and TAM frames the behavioral drivers of cybersecurity adoption.

2.4. Gaps in the Literature

Despite the growing global literature on cybersecurity, significant gaps remain in relation to developing countries, particularly in Africa.

- **Western-Centric Focus:** The majority of existing studies focus on enterprises in North America, Europe, and East Asia, where regulatory environments are mature and resource availability is higher (Anderson et al., 2020). This has produced a wealth of knowledge on best practices in advanced economies but leaves limited insight into contexts characterized by informality, weak governance, and constrained resources.
- **Neglect of SMEs:** While multinational corporations are often the focus of global cybersecurity research, SMEs, which represent over 80% of employment and a significant share of GDP in Africa, remain understudied. This is problematic given that SMEs face unique challenges, including limited budgets, informality, and a higher susceptibility to operational disruptions from cyberattacks (World Bank, 2020).
- **Limited Empirical Data:** Much of the existing literature on African cybersecurity relies on policy reports and anecdotal evidence rather than systematic empirical studies. There is a lack of large-scale surveys, longitudinal studies, and comparative analyses across different African regions.
- **Underexplored Theoretical Integration:** While frameworks such as IS risk management, RBV, and TAM have been widely applied in other contexts, their integration into cybersecurity research in Africa remains limited. This creates opportunities for theory-driven studies that contextualize global concepts in local realities.

By addressing these gaps, this study contributes to the literature by offering an empirical, theory-informed, and context-specific analysis of cybersecurity readiness among African enterprises.

3. Methodology

3.1. Research Design

This study employs a **qualitative multi-case analysis** research design, supplemented by secondary quantitative indicators. The choice of a multi-case approach is deliberate, as it allows for the exploration of similarities and differences across diverse enterprises while capturing the contextual realities of developing countries. Unlike single-case studies that provide depth but limited generalizability, a multi-case design enables a broader understanding of patterns, challenges, and readiness strategies across different African markets.

Where data availability permits, a **mixed-method element** is integrated through the inclusion of survey responses and numerical indices such as the ITU Global Cybersecurity Index (GCI). This enhances triangulation, allowing findings from interviews and policy analysis to be corroborated with quantitative evidence. The combination of qualitative and limited quantitative methods strengthens both the validity and reliability of the study.

The overarching research question guiding this study is:

How do enterprises in African developing countries perceive, implement, and align their cybersecurity practices with global standards such as NIST CSF and ISO/IEC 27001, and what scalable strategies can be recommended to strengthen readiness?

To address this, the research is structured around three objectives: identifying key risks, assessing readiness frameworks, and recommending defense strategies.

3.2. Case Selection

The study focuses on enterprises in **three African countries** representing varying levels of digital maturity and regulatory development:

- **Nigeria** – Africa's largest economy and a hub for fintech innovation, but with fragmented regulatory enforcement and frequent cybercrime incidents.
- **Kenya** – Recognized for mobile money adoption (e.g., M-Pesa), with an active regulatory environment but persistent cyber vulnerabilities.
- **South Africa** – One of the continent's more advanced digital economies, with stronger legal frameworks such as the Protection of Personal Information Act (POPIA), but also facing significant cyberattacks targeting its financial sector.

These countries were selected purposively to provide comparative insights: Nigeria illustrates the challenges of scale and informality, Kenya reflects rapid digital inclusion in a resource-limited environment, and South Africa represents the relatively advanced but still vulnerable end of the spectrum.

Within each country, a small sample of enterprises (n=3–5 per country) is included, focusing on SMEs in sectors such as **financial services, e-commerce, and logistics**. These sectors are chosen because they are at the forefront of digital adoption and disproportionately exposed to cyber threats.

3.3. Data Sources

The study draws on multiple sources of data to enhance credibility and triangulation:

- **Policy and Regulatory Documents:**

National cybersecurity strategies, data protection laws, and sector-specific guidelines issued by government regulators in Nigeria, Kenya, and South Africa.

- **Secondary Data:**

Existing reports and indices such as:

  - ITU Global Cybersecurity Index (GCI) – for benchmarking national-level readiness.
  - World Bank enterprise surveys – for contextualizing SME adoption of digital tools.
  - Reports by consulting firms (e.g., Deloitte, PwC) and industry associations highlighting regional cyber trends.

- **Structured Interviews:**

Semi-structured interviews with enterprise managers, IT leads, and policymakers. The interviews focus on practices, perceptions, and barriers to cybersecurity readiness. The semi-structured format balances flexibility with comparability across cases.

- **Survey Data (if feasible):**

Short questionnaires distributed to SMEs to capture perceptions of risks, budget allocations, and adoption of cybersecurity practices. This provides quantitative complementarity to qualitative findings.

The integration of these sources ensures a **rich, multi-layered dataset**, combining the policy environment, enterprise-level practices, and external expert assessments.

3.4. Data Collection Procedures

Document Review: Policy documents and reports were systematically collected from government portals, regional organizations (e.g., African Union, ECOWAS, SADC), and international agencies. These documents were analyzed to extract provisions on enterprise cybersecurity obligations, enforcement mechanisms, and institutional frameworks.

Interviews: Potential participants were identified through professional networks, business associations, and regulatory bodies. Interviews were conducted via video conferencing tools due to geographical spread and were recorded (with consent) for transcription. Each interview lasted 45–60 minutes, guided by a standardized question set that covered risk awareness, governance practices, technological controls, and perceptions of regulatory frameworks.

Secondary Indices: Data from the ITU GCI and similar indices were extracted for the three countries to provide a comparative baseline. These indices were cross-checked with qualitative findings to highlight consistencies or discrepancies.

Ethical Considerations: Ethical clearance was sought from an institutional review board (IRB). Participation was voluntary, informed consent was obtained, and confidentiality was guaranteed. Identifying details of enterprises and individuals were anonymized to prevent reputational harm.

3.5. Analytical Framework

The analysis proceeds in three stages:

- **Within-Case Analysis:**

Each enterprise case is analyzed individually to map risks, current practices, and regulatory context. Data is coded thematically based on key categories such as “governance,” “technical controls,” “awareness,” and “resource constraints.”

- **Cross-Case Comparison:**

Cases are compared across Nigeria, Kenya, and South Africa to identify similarities, differences, and patterns. For example, contrasts may emerge between fintech startups in Nigeria and e-commerce SMEs in Kenya regarding investment priorities and staff training.

- **Benchmarking Against Global Standards:**

Local practices are systematically compared to global frameworks such as NIST CSF and ISO/IEC 27001. For instance:

- **Identify:** Do enterprises conduct regular risk assessments?
- **Protect:** What preventive controls (e.g., firewalls, encryption, access management) are in place?
- **Detect:** Are intrusion detection systems and monitoring mechanisms used?
- **Respond:** Do enterprises have incident response protocols?
- **Recover:** Are backup and disaster recovery plans in place?

This benchmarking enables a structured evaluation of **gaps between local practices and global expectations**. Where enterprises align with global frameworks, best practices are documented; where they diverge, contextual barriers (e.g., cost, expertise) are analyzed.

3.6. Rigor and Validity

To ensure credibility and rigor:

- **Triangulation** is achieved by combining policy analysis, interviews, and indices.
- **Member checking** is conducted by sharing findings with selected interviewees for validation.
- **Thick description** ensures that findings are embedded in contextual realities, improving transferability to similar settings.
- **Reliability** is strengthened by using a standardized interview guide and coding framework.

3.7. Limitations of the Methodology

While robust, the methodology is subject to limitations. The reliance on purposive sampling limits generalizability, though it enhances depth and contextual sensitivity. Access to enterprises may also be constrained by willingness to disclose cybersecurity practices, given reputational risks. Finally, secondary indices such as the ITU GCI provide national-level insights but may not capture nuances at the enterprise level. These limitations are acknowledged and addressed through triangulation and careful interpretation of results.

3.8. Conclusion of Methodology

By combining a qualitative multi-case approach with policy analysis and readiness indices, this methodology provides a **comprehensive and context-sensitive lens** on cybersecurity readiness in African enterprises. The comparative benchmarking against global frameworks ensures that findings are not only descriptive but also evaluative, enabling actionable recommendations.

4. Results

4.1. Cyber Risks Identified

The findings reveal that African enterprises, particularly SMEs, face a constellation of cyber risks that mirror global threat trends but are exacerbated by contextual vulnerabilities.

4.1.1. Phishing and Social Engineering Attacks.

Phishing remains one of the most pervasive threats. Across all cases studied, enterprise managers reported incidents in which employees received fraudulent emails or SMS messages attempting to extract credentials. In Nigeria, phishing has become particularly acute in fintech environments, where criminals impersonate mobile money platforms and banks to steal customer data. The lack of robust employee awareness programs and multifactor authentication makes SMEs highly susceptible.

4.1.2. Ransomware and Malware Infections

Enterprises also face growing exposure to ransomware attacks. Several Kenyan SMEs in the logistics and retail sector reported system lockouts that halted operations for days until systems were rebuilt from scratch. While global ransomware syndicates target multinational corporations, African SMEs are often victims of opportunistic campaigns exploiting unpatched systems and outdated antivirus solutions. Limited incident response capabilities further increase the operational and financial damage.

4.1.3. Insider Threats

Insider risks malicious or accidental were widely acknowledged by respondents. In South African enterprises, interviewees cited cases of disgruntled employees leaking sensitive information or misusing access privileges. In Nigeria and Kenya, accidental data leaks due to weak access controls and insufficient staff training were more common. These insider-related vulnerabilities are particularly severe in SMEs, which often lack segregation of duties or monitoring tools.

4.1.4. Cloud Vulnerabilities and Third-Party Risks.

With the rapid adoption of cloud services, SMEs have increasingly outsourced data storage and applications to vendors such as AWS, Microsoft Azure, and regional providers. While this provides scalability, it introduces dependencies on third-party security practices. Nigerian fintechs, for example, acknowledged that they rely almost entirely on their vendors for security, with little capacity to audit compliance. Similarly, e-commerce firms in Kenya highlighted the risks of vendor lock-in, where migrating data to new providers is costly and complex.

Collectively, these risks underscore a dual vulnerability: African enterprises face both the **universal risks of digitization** and **context-specific challenges** that amplify the likelihood and impact of incidents.

4.2. Current Readiness

Across the three countries examined, enterprise readiness was consistently low relative to global benchmarks. Findings indicate reliance on ad-hoc measures, low awareness training, and weak incident response mechanisms.

4.2.1. Ad-Hoc Security Tools

Most SMEs lack structured cybersecurity frameworks and instead depend on basic tools such as antivirus software and firewalls. In Nigeria, fintech startups typically deploy off-the-shelf endpoint protection, but few integrate monitoring or threat intelligence feeds. In Kenya, small logistics firms often rely on free or low-cost antivirus solutions with limited updates. South African enterprises showed higher levels of investment, but these were uneven across sectors.

4.2.2. Low Awareness Training

A critical gap identified is the lack of employee awareness. Across all cases, respondents acknowledged that most cyber incidents originated from human error employees clicking malicious links, using weak passwords, or failing to follow basic protocols. However, only a minority of SMEs conducted regular cybersecurity training. Those that did often relied on generic online modules rather than tailored programs contextualized to their industry risks.

4.2.3. Weak Incident Response

Incident response capabilities remain underdeveloped. Few SMEs maintain formal incident response plans or conduct tabletop exercises. Nigerian fintechs reported that when breaches occurred, they relied on informal WhatsApp groups to coordinate responses rather than established protocols. In Kenya, SMEs often chose to "wipe and rebuild" systems after malware incidents rather than investigate root causes. South African enterprises were more likely to have structured response teams, but even here, the level of preparedness fell short of ISO or NIST standards.

4.2.4. Compliance-Oriented Readiness

In some cases, particularly in South Africa, readiness was driven by compliance with regulations such as the Protection of Personal Information Act (POPIA). However, compliance was often superficial focused on documentation rather than substantive technical measures. This reflects a global pattern where compliance is treated as an end in itself rather than a baseline for holistic cybersecurity readiness.

Overall, readiness in African SMEs is characterized by a **reactive posture**: enterprises respond after incidents occur rather than adopting proactive risk management.

4.3. Comparative Analysis: Readiness Scorecard vs. Global Benchmarks

To evaluate readiness systematically, local enterprise practices were compared against the **NIST Cybersecurity Framework (CSF)** and **ISO/IEC 27001**. A readiness scorecard was developed, rating practices in the five NIST CSF categories Identify, Protect, Detect, Respond, and Recover on a scale of **High, Medium, Low** relative to international expectations.

4.3.1. Identify (Asset Management & Risk Assessment)

Most SMEs scored **Low**. Few conducted formal asset inventories or risk assessments. Business owners often had limited awareness of critical assets or dependencies on third parties. In contrast, global best practice requires continuous risk assessment and mapping of assets.

4.3.2. Protect (Safeguards)

Enterprises typically scored **Medium-Low**. Basic safeguards such as antivirus software and firewalls were in place, but advanced controls like encryption, multi-factor authentication, and role-based access were inconsistently applied. South African enterprises showed higher alignment, particularly in regulated industries.

4.3.3. Detect (Monitoring)

Scores were consistently **Low**. Few SMEs deployed intrusion detection systems, log monitoring, or anomaly detection. Instead, detection often occurred only when a disruption was visible (e.g., system outages). This contrasts with global benchmarks where proactive monitoring is central.

4.3.4. Respond (Incident Management)

Enterprises scored **Low** overall. Structured response teams and communication protocols were rare. Most SMEs relied on external consultants during crises. By comparison, global standards emphasize pre-planned, rehearsed response capabilities.

4.3.5. Recover (Resilience and Continuity)

Recovery practices scored **Medium-Low**. While some SMEs maintained data backups, these were often manual, infrequent, and not tested for integrity. Few had disaster recovery sites or redundancy. Global standards recommend tested backup systems and continuity planning.

The comparative analysis highlights significant gaps. Even South Africa, the most advanced among the three cases, fell below global benchmarks in detection and incident response. Nigeria and Kenya lagged even further behind, particularly in governance and risk assessment.

4.4. Case Illustrations

4.4.1. Nigeria: Fintech Sector

Nigeria's booming fintech industry exemplifies both opportunity and vulnerability. Startups such as Flutterwave and Paystack have expanded rapidly, handling billions in transactions. Yet, smaller fintechs interviewed admitted they struggled to implement comprehensive cybersecurity measures. One IT manager reported that phishing attempts targeting their customer base occurred weekly, yet most employees lacked formal training to recognize such attacks. Another fintech noted that their reliance on third-party cloud vendors left them uncertain about compliance with global standards. This underscores the challenge of scale rapid growth outpaces the development of internal security infrastructure.

4.4.2. Kenya: E-Commerce and Logistics SMEs

In Kenya, SMEs in the e-commerce and logistics sectors provided illustrative cases. One logistics startup reported that a ransomware attack in 2021 locked them out of critical systems for three days, halting deliveries and costing significant revenue. Lacking an incident response plan, they resorted to re-installing their systems without investigating the breach vector. Similarly, e-commerce firms described frequent fraud attempts involving stolen credit cards. While some adopted payment gateways with fraud detection, many lacked back-end monitoring, relying instead on banks to flag suspicious transactions. These cases highlight a **reactive, fragmented approach** to cybersecurity readiness.

4.4.3. South Africa: Traditional SMEs under POPIA

South African SMEs displayed relatively stronger practices, largely due to regulatory requirements under POPIA. For example, a mid-sized law firm interviewed had adopted encryption for client records and conducted annual staff training. However, even here, gaps remained in monitoring and incident response. Another case a retail SME treated compliance as a "tick-box" exercise, outsourcing most of its IT security to a vendor without conducting audits. While regulation drove higher awareness, actual technical readiness varied significantly by sector and resources.

4.5. Summary of Findings

- **Risks Identified:** Phishing, ransomware, insider threats, and cloud vulnerabilities dominate the threat landscape.
- **Current Readiness:** SMEs rely on ad-hoc tools, have low staff awareness, and lack structured incident response.
- **Comparative Analysis:** All three countries fall below global benchmarks, with South Africa ahead but still deficient in detection and response.
- **Case Insights:** Nigerian fintechs face phishing and vendor risks; Kenyan SMEs face ransomware and fraud challenges; South African SMEs are more compliance-driven but uneven in practice.

These findings underscore the need for scalable, context-sensitive defense strategies. While global frameworks provide strong guidance, African enterprises require tailored approaches that account for resource limitations, regulatory fragmentation, and workforce shortages.

5. Discussion

5.1. Comparative Patterns in Emerging Economies

The findings from Nigeria, Kenya, and South Africa demonstrate a fragmented yet gradually evolving landscape of cybersecurity readiness in Africa. To place these insights into perspective, it is useful to compare them with other emerging economies where rapid digitalization has also transformed business practices.

5.1.1. Kenya's M-Pesa vs. India's Unified Payments Interface (UPI).

Kenya's M-Pesa has long been celebrated as a pioneering mobile money system that revolutionized financial inclusion in Africa. However, while M-Pesa enabled millions of unbanked citizens to participate in the digital economy, it also introduced systemic risks. Fraud, SIM-swapping, and identity theft became widespread, with SMEs particularly vulnerable due to weak verification and monitoring mechanisms (Mbiti & Weil, 2016). In contrast, India's UPI, launched in 2016, adopted a more centralized, government-backed model, integrating banks, regulators, and fintechs into a unified payment system. UPI has witnessed exponential growth, surpassing $1 trillion in annual transactions by 2022 (RBI, 2022). Importantly, India embedded cybersecurity into the system through regulatory oversight, mandatory two-factor authentication, and real-time fraud monitoring. Compared to Kenya, India's ecosystem demonstrates how strong institutional coordination and regulatory enforcement can significantly enhance cyber resilience, even in a resource-constrained environment.

5.1.2. Brazil's PIX vs. African E-Payment Systems.

Brazil's PIX instant payment system, introduced in 2020, provides another point of contrast. PIX is government-owned and centrally regulated by the Central Bank of Brazil, ensuring uniform security standards across financial institutions. While Brazil faces its own challenges of fraud and phishing, the centralized infrastructure has allowed for rapid incident response and policy-driven adjustments. African fintech systems, by contrast, are more fragmented, with multiple private actors developing mobile wallets and e-commerce platforms in parallel, often without harmonized security standards. The lack of central oversight leaves SMEs more exposed to varying levels of vendor security and weak incident reporting mechanisms.

These comparisons illustrate two critical lessons: first, that **institutional coordination** is a decisive factor in cyber readiness, and second, that **regulation embedded at the design stage of digital platforms** enhances resilience. While African innovations like M-Pesa demonstrated the potential of leapfrogging traditional financial systems, they also highlight the risks of rapid adoption without proportionate investment in governance and security.

5.2. Theoretical Implications: Cyber Readiness as a Capability under RBV

The results also yield important theoretical implications when interpreted through the **Resource-Based View (RBV)** of the firm. RBV posits that sustainable competitive advantage arises when firms possess resources and capabilities that are valuable, rare, inimitable, and non-substitutable (Barney, 1991). Applying RBV to cybersecurity reframes readiness not simply as a compliance activity but as a **strategic capability** that differentiates resilient enterprises from vulnerable ones.

For African SMEs, cybersecurity readiness can serve as a valuable capability. In increasingly digitized markets, customer trust is contingent on secure transactions, data protection, and continuity of service. Firms that invest in cybersecurity

even at basic levels, such as encryption, multifactor authentication, and employee training, signal credibility to customers, regulators, and investors. This, in turn, enables access to new markets, partnerships, and funding opportunities.

However, the rarity and inimitability of such capabilities in African SMEs are constrained. Skilled cybersecurity professionals are scarce, leading to a reliance on external vendors. Financial constraints prevent SMEs from adopting enterprise-grade tools or certifications like ISO/IEC 27001. Consequently, while some firms may temporarily differentiate themselves through better cybersecurity practices, the sustainability of such advantages remains uncertain unless structural constraints (e.g., workforce and resource gaps) are addressed.

Nevertheless, the RBV framework highlights an important shift: African SMEs must transition from viewing cybersecurity as a **cost center** to recognizing it as a **capability that creates competitive advantage**. In this framing, readiness is not only about avoiding losses from cyberattacks but also about enabling strategic growth in globalized digital markets.

5.3. Policy Implications

The study highlights several policy imperatives critical for improving cybersecurity readiness in developing regions:

5.3.1. Digital Literacy and Awareness

One of the most pressing gaps identified is low employee awareness of cyber risks. Governments, industry associations, and NGOs can play a role in promoting digital literacy programs targeted at SMEs. National awareness campaigns, similar to India's cybersecurity awareness drives, can help instill basic practices such as password hygiene, phishing recognition, and safe digital behavior. Moreover, incorporating cybersecurity modules into vocational and university curricula can help build a pipeline of skilled professionals.

5.3.2. Regulatory Harmonization and Enforcement

Regulatory fragmentation emerged as a major barrier. Unlike the EU's GDPR, African nations often lack harmonized frameworks that provide clear expectations and enforcement mechanisms. Policymakers should work toward regional harmonization through bodies such as the African Union, developing continent-wide minimum cybersecurity standards. Stronger enforcement capacity through national Computer Emergency Response Teams (CERTs), data protection authorities, and sector-specific regulators will be necessary to ensure compliance and accountability.

5.3.3. Workforce Development

The shortage of cybersecurity professionals is perhaps the most structural challenge. Governments can incentivize training through scholarships, professional certification subsidies, and partnerships with private training providers. Regional centers of excellence could be established to train cybersecurity experts who can then support SMEs across multiple countries. International organizations (e.g., World Bank, ITU) can also play a role in funding workforce development initiatives.

5.3.4. Public-Private Partnerships

Given resource constraints, African governments cannot shoulder the burden alone. Partnerships between government agencies, telecom operators, cloud service providers, and industry associations are critical. For example, Brazil's PIX demonstrated how public-private collaboration can create secure and inclusive payment systems. Similar partnerships in Africa could help SMEs access subsidized cloud security services or shared incident response platforms.

5.4. Business Implications

For SMEs, the findings underline an urgent need to reconceptualize cybersecurity not as an afterthought or regulatory burden but as a **strategic enabler of growth**. Several implications emerge:

5.4.1. Cybersecurity as Customer Trust

Consumers are increasingly aware of data privacy and fraud risks. Enterprises that can demonstrate strong security practices are more likely to earn trust, retain customers, and attract investment. For fintechs, e-commerce, and professional services firms, security is no longer optional it is part of the value proposition.

5.4.2. Cost-Effective Readiness Strategies

SMEs often perceive cybersecurity as prohibitively expensive. However, the findings suggest that even **low-cost, high-impact measures** such as employee training, enforcing strong authentication, and maintaining regular backups can significantly reduce risk. SMEs must prioritize resource allocation, adopting incremental improvements rather than waiting for comprehensive but unaffordable solutions.

5.4.3. Leveraging Cloud and Shared Services

While reliance on cloud vendors poses risks, it also provides opportunities for SMEs to access enterprise-grade security at scale. By negotiating service-level agreements that explicitly include security responsibilities, SMEs can enhance readiness without building in-house capabilities. Industry associations can further negotiate collective contracts with providers, lowering costs for members.

5.4.4. Integration of Cybersecurity into Business Strategy

Finally, SMEs must integrate cybersecurity into broader business planning. Rather than treating it as a separate IT issue, cybersecurity should be embedded in governance, risk management, and operational continuity. This requires leadership buy-in, board-level oversight, and the recognition that resilience is as important as innovation.

5.5. Toward a Context-Sensitive Model of Cyber Readiness

Synthesizing the findings, comparisons, and theoretical insights, it is clear that African SMEs cannot simply import global frameworks wholesale. Instead, a **context-sensitive model of cyber readiness** is needed one that aligns with NIST and ISO principles but adapts them to resource-constrained environments. Key features of such a model include:

- Prioritization of **basic controls** (e.g., authentication, backups, employee training) as foundational layers.
- **Phased adoption** of advanced measures as resources allow.
- Leveraging **regional cooperation** (e.g., African Union CERT networks) to share threat intelligence and resources.
- Embedding cybersecurity into **national digital strategies**, ensuring that enterprises see readiness as integral to competitiveness.

This hybrid approach acknowledges the realities of limited resources while striving for alignment with global standards.

5.6. Conclusion of Discussion

The comparison with India's UPI and Brazil's PIX demonstrates that institutional coordination and early integration of security are decisive in building resilient digital economies. African enterprises, however, continue to operate in fragmented ecosystems where resource constraints and regulatory gaps exacerbate vulnerabilities.

From a theoretical standpoint, the Resource-Based View reframes cybersecurity readiness as a strategic capability that can enhance competitiveness rather than a mere cost. Policymakers must prioritize digital literacy, harmonized regulations, and workforce development, while SMEs must adopt incremental, cost-effective measures and embed cybersecurity into their business strategies.

Ultimately, cybersecurity in African SMEs must evolve from a **reactive, ad-hoc posture** to a **proactive, strategic enabler of trust and growth**. Only then can developing economies fully harness the benefits of digitalization while mitigating its inherent risks.

6. Conclusion

The rapid digitalization of developing economies has opened new avenues for economic growth, inclusion, and competitiveness, yet it has also introduced heightened vulnerability to cyber threats. This study investigated the **cybersecurity readiness of African enterprises**, with a particular focus on small and medium-sized enterprises (SMEs) in Nigeria, Kenya, and South Africa. By examining cyber risks, evaluating readiness frameworks against global standards, and comparing patterns with other emerging economies, the study has provided insights into both the opportunities and the shortcomings of current cybersecurity practices in developing contexts.

6.1. Restating Major Findings

The research revealed that **cyber risks facing African enterprises are multidimensional**. Phishing, ransomware, insider threats, and cloud vulnerabilities were identified as dominant threats. While these risks are not unique to Africa, their impact is amplified by contextual realities such as limited awareness, fragmented regulations, and overreliance on external vendors.

The readiness of enterprises to manage these risks was found to be **low relative to global benchmarks**. Most SMEs employ ad-hoc measures such as antivirus software and basic firewalls but lack structured governance, monitoring, and incident response mechanisms. Training and awareness remain particularly weak, leaving human error as a consistent entry point for attackers. Recovery practices exist but are inconsistently tested and often fail to meet the standards set by frameworks such as the NIST Cybersecurity Framework or ISO/IEC 27001.

The comparative analysis further highlighted stark differences between African enterprises and global best practices. While South Africa's relatively stronger regulatory environment (e.g., POPIA) has driven some progress, significant gaps remain, particularly in detection and incident response. Nigeria and Kenya, despite being digital innovation hubs, show persistent weaknesses in governance and preparedness. Compared with India's UPI and Brazil's PIX, Africa's digital ecosystems remain **fragmented**, lacking the institutional coordination and embedded regulatory oversight that have enabled other emerging economies to balance growth with security.

6.2. Contributions to IS Risk Management and Cybersecurity Readiness

This study makes several contributions to academic debates in **Information Systems (IS) risk management** and **cybersecurity readiness**.

First, it demonstrates the importance of contextualizing global frameworks within resource-constrained environments. IS risk management literature often assumes the availability of technical capacity, skilled personnel, and strong institutions. By examining African SMEs, this study highlights how risk management unfolds in settings where such assumptions do not hold, thus expanding the scope of IS research into underexplored contexts.

Second, the research applies the **Resource-Based View (RBV)** to cybersecurity, reframing readiness as a potential source of competitive advantage rather than merely a compliance function. This perspective underscores that enterprises capable of building resilience through trust, governance, and strategic security investments can differentiate themselves in increasingly digitalized markets. Cyber readiness, therefore, is not simply defensive but can be strategically enabling.

Third, the findings intersect with the **Technology Acceptance Model (TAM)**, showing how perceptions of complexity and usefulness shape SME adoption of cybersecurity tools. The study suggests that SMEs are more likely to embrace security measures when they are affordable, easy to implement, and embedded within existing digital platforms. This insight contributes to adoption research by highlighting behavioral and cultural dimensions of readiness, particularly in developing-world contexts.

Finally, at the policy level, the study provides evidence to support **regional harmonization of cybersecurity frameworks** and investments in workforce development. It demonstrates that African SMEs cannot simply import global models but require tailored, incremental approaches aligned with local realities.

6.3. Limitations

Despite its contributions, this study is subject to several limitations.

First, the research focused on **three African contexts Nigeria, Kenya, and South Africa **which, while illustrative, do not capture the full diversity of the continent. Countries with lower levels of digital penetration, weaker institutions, or ongoing conflict may face even greater challenges not reflected in these cases. Future research should expand the scope to include a wider set of African economies and conduct comparative analyses across regions such as West, East, and Southern Africa.

Second, the analysis relied on a combination of **secondary data sources, policy reports, and structured interviews**. While this triangulation strengthens credibility, it also introduces limitations. National-level indices such as the ITU Global Cybersecurity Index provide useful benchmarks but may not reflect enterprise-level realities with precision.

Similarly, reliance on policy documents means that the study captures intended frameworks but not always their practical implementation.

Third, access to SMEs proved challenging, given the sensitivity of cybersecurity disclosures. Many enterprises were unwilling to share detailed information about breaches or vulnerabilities. As a result, some findings are based on self-reports that may be subject to underreporting bias. Future research could address this by employing anonymous surveys or collaborating with industry associations to encourage openness.

Finally, the research design emphasized qualitative analysis supported by selected quantitative indicators. While this approach provides rich insights, it limits generalizability. Future studies could incorporate large-scale surveys or longitudinal designs to measure changes in readiness over time and test causal relationships more systematically.

6.4. Concluding Thoughts

Despite these limitations, the study underscores the urgent need to **reframe cybersecurity in African SMEs from a reactive posture to a proactive, strategic capability**. Cyber threats will only intensify as digital adoption accelerates, making readiness a prerequisite for resilience, competitiveness, and trust. African enterprises must move beyond ad-hoc tools toward integrated risk management, supported by regulatory harmonization, digital literacy initiatives, and workforce development.

At the same time, policymakers and international organizations must recognize that **global cybersecurity resilience depends on inclusive progress**. Cyber threats are transnational, and vulnerabilities in one region can reverberate globally. Thus, strengthening cybersecurity readiness in Africa is not only a local imperative but also a contribution to global digital stability.

In conclusion, this study fills a significant gap in the literature by situating African SMEs within global cybersecurity debates, integrating IS risk management with RBV and TAM, and providing context-sensitive recommendations. It invites scholars, practitioners, and policymakers to rethink cybersecurity readiness not as a luxury of developed economies but as a **universal necessity** for enterprises navigating an increasingly interconnected world.

References

[1] Ahmed, G., & Amany. (2024). Cyber insecurity effect on the economy of Africa. OI-JET. In OI-Journal of Emerging Technologies, December. Retrieved from https://journals.ekb.eg/article_446966_666fbd18c58db4f2edc06b398fe597ab.pdf EKB Journals

[2] Interpol. (2025). INTERPOL Africa cyberthreat assessment report. INTERPOL. Retrieved from INTERPOL site (ransomware detections across Africa in 2024) Interpol

[3] Kearney. (2022). Cybersecurity in Africa—a call to action. Kearney. Retrieved from https://www.kearney.com/... HSRC+5Kearney+5EKB Journals+5

[4] KPMG Africa. (2022). Africa Cyber Security Outlook. KPMG. Retrieved from https://assets.kpmg.com/... MDPI+15KPMG Assets+15arXiv+15

[5] Mwangi, K. (2025, February 13). Best practices for SME cybersecurity in Africa. Techinafrica. Retrieved from https://www.techinafrica.com/... journals.eanso.org+15Tech In Africa+15KPMG Assets+15

[6] Mutuku, M., & Muathe, S. (2025). Has increased digitisation of services led to more cyber exposure? A desk review. East African Journal of Information Technology, 8(1), 320–326. https://doi.org/10.37284/eajit.8.1.3283 journals.eanso.org+1

[7] Pawar, S. (2022). A framework for least cybersecurity controls to be adopted. Journal of Cybersecurity in Developing Nations, 2022 edition. Retrieved from https://www.sciencedirect.com/... ScienceDirect

[8] Rombaldo Junior, C., Becker, I., & Johnson, S. (2023). Unaware, Unfunded and Uneducated: A systematic review of SME cybersecurity. arXiv Preprint. Retrieved from https://arxiv.org/abs/2309.17186 arXiv+1

[9] Security & Trust in Africa's Digital Financial Inclusion Landscape. (2024, March 8). Carnegie Endowment for International Peace. Retrieved from https://carnegieendowment.org/... Carnegie Endowment

[10] Systematic Review of SME Cybersecurity. (2023). arXiv Preprint. Retrieved from https://arxiv.org/pdf/2309.17186 arXiv+1

[11] Liquid Intelligent Technologies. (2021). The evolving cyber security threat in Africa. Liquid. Retrieved from https://liquid.tech/... Liquid Intelligent Technologies

[12] Khan, N. (2025). Investigating the experiences of providing cybersecurity... Computers & Security. Retrieved from https://www.sciencedirect.com/... ScienceDirect

[13] Barney, J. (1991). Firm resources and sustained competitive advantage. Journal of Management, 17(1), 99–120. [Classic RBV foundational work] en.wikipedia.org