© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716597

Cybersecurity Threats in Nigerian Banks: Implications for Human Security and Strategic Responses in the 21st Century

TAELOLU, OMOTUNDE OLUWASESAN[1], PROF. ISIAKA ALANI BADMUS[2], DR. OGUNDELE A.T.[3]

[1, 2, 3]*Department of Peace, Conflict and Strategic Studies College of Social and Management Sciences, Afe Babalola University, Ado-Ekiti*

Abstract - Nigeria's banking sector has undergone rapid digitalisation, driven by the Central Bank of Nigeria's cashless economy policies and pandemic-accelerated adoption, significantly expanding the attack surface available to cybercriminals. Despite a growing cybersecurity literature, the intersection of cyber threats with human security within the Nigerian context remains critically underexplored. This study examines cybersecurity threats facing Tier-1 commercial banks in Lagos State, analyses their human security implications, and evaluates strategic mitigation responses. Employing a cross-sectional survey design, 460 respondents comprising 230 bank staff and 230 customers were sampled from First Bank of Nigeria, United Bank for Africa, Guaranty Trust Bank, Access Bank, and Zenith Bank. Data were analysed using descriptive statistics, Pearson correlation, regression analysis, and ANOVA, within a dual theoretical framework integrating Risk Management Theory and Systems Theory. Findings confirm a severe threat environment, with mobile banking expansion identified as the primary vulnerability catalyst (M=3.62), alongside phishing, ransomware, DDoS attacks, and high insider threat perception (M=3.59). Cyberattacks were found to erode customer confidence (M=3.60), disrupt financial services for vulnerable populations (M=3.59), and impose significant psychological pressure on employees (M=4.02), empirically validating cybersecurity as a human security issue. While banks demonstrate strong multi-factor authentication adoption (M=4.05), a critical Effectiveness Paradox emerges: customers feel secure (M=4.09), yet attack frequency remains largely unreduced (M=2.97). An Expertise Paradox further revealed that IT and risk professionals hold significantly lower confidence in security measures than operational staff. The study repositions cybersecurity as a macro-prudential and social equity imperative, recommending Zero Trust architecture, AI-driven threat analytics, mandated inter-institutional intelligence sharing, and national digital literacy campaigns.

Keywords: cybersecurity, Nigerian banking sector, human security, strategic responses, digital financial inclusion, cyber resilience, emerging economies

I. INTRODUCTION

Banking has never been static. Across centuries, it has evolved in response to commerce, regulation, and technology. Yet few transformations have been as rapid or as consequential as the shift to digital operations that has unfolded over the past two decades. Today, financial institutions process payments, manage records, extend credit, and engage customers almost entirely through electronic platforms. The efficiency gains have been substantial. So, too, have the vulnerabilities. As banks have embedded themselves deeper into digital infrastructure, they have simultaneously expanded the surface area available to criminal exploitation. Phishing campaigns, ransomware attacks, data breaches, identity fraud, insider threats, and unauthorised system intrusions are now routine features of the financial landscape rather than exceptional events (Natalucci et al., 2024; Obi et al., 2024). What was once a concern confined to information technology departments has become a matter with consequences for service continuity, customer confidence, institutional reputation, and in extreme cases, macroeconomic stability (Wu et al., 2023). The scale of this problem at the global level is difficult to overstate. Criminal networks, and in some instances state-affiliated actors, have demonstrated both the capability and the intent to target financial systems at their most vulnerable points, including payment gateways, customer databases, internal communication systems, and human behaviour itself. Malekos Smith et al. (2020) estimated global cybercrime losses at approximately USD 945 billion in 2020, and the World Economic Forum (2023) projected that figure could exceed USD 10.5 trillion

annually by 2025. These are not merely statistics about technical failures. They reflect the growing recognition that cybersecurity in banking is a matter of strategic governance, economic resilience, and public trust, not a problem to be resolved within server rooms alone. Nigeria presents a particularly compelling case for examining this challenge. Over the last decade, the country's banking sector has undergone substantial digital transformation. The spread of mobile banking, electronic transfers, card payment systems, and fintech-integrated platforms has significantly broadened financial access and improved operational reach. But this expansion has not come without cost. Nigerian banks and their customers have experienced a notable rise in cyber-enabled incidents, ranging from social engineering and phishing to malware deployment and unauthorised withdrawals. The 2024 attack on Hope Payment Service Bank, which reportedly resulted in losses of approximately ₦10 billion, serves as a prominent illustration of what is at stake (Adeniyi, 2024). More broadly, electronic fraud cases rose by 45% between 2020 and 2024 (NeFF, 2024), and over 1.3 million phishing attempts were recorded against bank customers in the first six months of 2023 alone (Agwulonu & Ijaseun, 2024). These figures point not to isolated incidents but to a sustained and escalating pattern of threat.

A key contextual factor shaping this environment is the Central Bank of Nigeria's cashless policy. First introduced in 2012 and reinforced through subsequent reforms, the policy sought to reduce cash dependency, stimulate electronic payment adoption, and modernise Nigeria's financial architecture (CBN, 2020). Its intentions have largely been realised in terms of transaction growth and system modernisation. However, the increased dependence on digital channels that the policy has produced has also widened the range of entry points available to cybercriminals. This dynamic intensified during the COVID-19 pandemic, as remote banking and contactless payments became necessities rather than preferences. In many respects, digital adoption outpaced the development of the security frameworks, customer literacy, and regulatory enforcement mechanisms needed to support it safely (Fadare et al., 2023). The result is a financial sector in which technological advancement and security fragility coexist in uncomfortable proximity.

What is often missing from the existing scholarship on this subject is an adequate account of the human dimension. Much of the literature on banking cybersecurity centres on technical vulnerabilities, financial losses, operational risk, and institutional response mechanisms. These are legitimate areas of inquiry, but they tend to leave out the people on the other side of the transaction screen. In developing economies such as Nigeria, digital banking is not merely a convenient alternative to branch visits. For millions of individuals and small businesses, it is the primary means through which salaries are received, household bills are settled, school fees are paid, and commercial obligations are met (Björck et al., 2015; O'Connell, 2020). When cyber incidents disrupt these services or compromise these accounts, the consequences extend well beyond operational inconvenience. They manifest as financial hardship, psychological distress, eroded trust in formal financial institutions, and a diminished sense of security in everyday economic life.

These wider consequences become clearer when examined through the framework of human security. Originally articulated by the United Nations Development Programme (1994), human security identifies seven interconnected dimensions of individual and collective well-being: economic, food, health, environmental, personal, community, and political security. Mahbub ul Haq (1995) argued influentially that security must be understood not solely as a state-centred concept, but as a condition rooted in people's freedom from fear and freedom from want. Applied to banking, this framework reveals that cyber threats can simultaneously undermine economic security through financial loss, personal security through fraud and identity compromise, community security through declining institutional trust, and political security through weakened confidence in regulatory systems. It provides an analytical lens that moves the conversation beyond technical risk management toward the broader social stakes of digital financial vulnerability. This broader perspective remains conspicuously absent from the Nigerian literature on banking cybersecurity. Studies conducted within the Nigerian context have tended to concentrate on fraud detection, internal controls, system weaknesses, and institutional risk mitigation. While such work has generated valuable insights, there remains limited empirical investigation into how cyber threats in major banks shape human security outcomes,

particularly in terms of economic stability, personal welfare, public trust, and social confidence in financial systems. There is also a notable absence of research focused specifically on the systemically important institutions that anchor Nigeria's formal banking sector and process a disproportionate share of its digital transactions.

This investigation is designed to address that gap. It focuses on the FUGAZ Tier-1 banks, First Bank of Nigeria, United Bank for Africa, Guaranty Trust Bank, Access Bank, and Zenith Bank, operating in Lagos State over the period 2017 to 2025. Lagos State is the appropriate setting given its status as Nigeria's commercial and financial hub, its high density of banking operations, and the concentration of digital financial activity within its boundaries. The FUGAZ banks are selected on account of their systemic significance, the breadth of their customer bases, and their centrality to Nigeria's financial architecture. Against this backdrop, the study examines the principal cybersecurity threats confronting these institutions, analyses their implications through the lens of human security, and evaluates the adequacy of the strategic responses that have been adopted in response. In doing so, it seeks to contribute a more complete picture of what cybersecurity in Nigerian banking means, not only for institutions, but for the people whose economic lives depend on them.

II. LITERATURE REVIEW

2.1 Conceptual Framework: Cybersecurity and Human Security.

Cybersecurity is a multidimensional field encompassing strategies, technologies, and practices to protect systems, networks, and data from threats ranging from unauthorised access to ransomware and DDoS attacks (Ruan et al., 2019). Scholars such as Hoffman et al. (2020) argue that viewing cybersecurity solely as a technological problem creates systems that are technically robust but socially and operationally fragile. The financial sector, as custodian of sensitive data and monetary assets, presents a particularly compelling case: the Nigeria Deposit Insurance Corporation (NDIC, 2021) and CBN (2022) have both acknowledged cybersecurity as critical to financial system stability.

Human security, as conceptualised by the United Nations Development Programme (UNDP, 1994), represents a paradigm shift from state-centred security to individual well-being, encompassing freedom from fear and freedom from want. Scholars such as Kaspersen and Lindsey (2014) argue that cyberattacks on banking institutions create widespread economic insecurity, particularly in developing economies where access to financial services is limited. Familoni and Shoetan (2024) extend this framing by situating financial cybercrime as a direct threat to human security, undermining economic stability and eroding trust in financial institutions. This study operationalises human security within the context of Nigerian banking cybersecurity, demonstrating how financial fraud, data breaches, and service disruptions compromise economic stability, personal well-being, and national trust.

2.2 Cybersecurity Threats in the Banking Sector

The landscape of cybersecurity threats has evolved substantially, from early insider-driven fraud in the 1960s and 1970s, through the rise of phishing and DDoS attacks in the internet era, to today's sophisticated ransomware, Advanced Persistent Threats (APTs), and artificial intelligence (AI)driven attacks (Wells, 2002; Lottu et al., 2023). A landmark example of systemic risk is the Carbanak APT campaign (2013–2015), in which cybercriminals infiltrated over 100 financial institutions globally, stealing an estimated USD 1 billion (Kaspersky, 2015). State-sponsored operations, exemplified by North Korea's Lazarus Group and the USD 81 million Bangladesh Bank heist in 2016 (Kim, 2022), further illustrate the geopolitical dimension of banking cybercrime.

In Nigeria, the threats mirror global trends but are exacerbated by specific contextual vulnerabilities. Ajufo and Qutieshat (2023) identified four key human-factor vulnerabilities in Nigerian banks, social engineering, poor password practices, security fatigue, and employee burnout, contributing to annual losses of between USD 4.1 million and USD 6.6 million. Reis et al. (2024) document a largely reactive posture, while Wang et al. (2020) found malware, spam, and hacking to be the primary threats, compounded by legislative non-compliance and outdated cybersecurity technologies. The CBN (2022) reported annual losses exceeding ₦127 billion from phishing, ransomware, and DDoS attacks. The

mobile banking revolution has introduced a new primary vector: Android-based devices, which dominate the Nigerian market, are particularly susceptible to data leakage and malicious applications (Nosrati & Bidgoli, 2016; Chen et al., 2020).

2.3 Regulatory and Comparative Frameworks

The effectiveness of cybersecurity is significantly shaped by regulatory environments. Developed economies demonstrate the value of stringent, comprehensive frameworks. The United States combines voluntary NIST Cybersecurity Framework guidelines with the Cybersecurity
Information Sharing Act (CISA, 2015), facilitating public-private threat intelligence sharing
(Dandurand & Serrano, 2013). The European Union's General Data Protection Regulation (GDPR, 2018) mandates strict data protection with penalties up to 4% of global revenue, compelling financial institutions worldwide to elevate their practices (Koops & Leenes, 2014).

Nigeria's primary instruments, the Cybercrimes (Prohibition, Prevention, etc.) Act (2015) and the CBN's Risk-Based Cybersecurity Framework (2018), provide a legal foundation, but limited enforcement capacity, budgetary constraints, and a shortage of cybersecurity professionals severely hamper their effectiveness (Onyekachi, 2024; Olukoya, 2022). The Nigeria Data
Protection Regulation (NDPR, 2019) complements these frameworks but remains inconsistently enforced. A comparative analysis reveals that while developed economies prioritise continuous risk assessment, mandatory information sharing, and capacity building, Nigerian banks often adopt a reactive posture, implementing controls after breaches rather than anticipating them (Reis et al., 2024; Takemura, 2022).

2.4 Strategic Responses and Their Limitations

Strategic responses to cybersecurity threats encompass technological investment, policy adjustment, and human resource development (Matsuura, 2016). Banks globally deploy encryption, multi-factor authentication (MFA), intrusion detection/prevention systems (IDS/IPS), and increasingly, AI-powered threat detection (Williams, 2017). Nigeria's NG-FinCERT, established by the CBN, represents an institutional effort at coordinating financial sector cybersecurity responses (CBN, 2019). However, the literature consistently identifies critical weaknesses: over-reliance on visible, compliance-driven controls, insufficient data encryption, weak public-private partnerships, and reactive rather than proactive threat management (Adegbite et al., 2023; Hassan et al., 2024). Siponen and Vance (2010) caution that robust technical defences are undermined without corresponding investments in organisational culture, employee training, and cybersecurity awareness, a finding particularly resonant in the Nigerian context.

2.5 Theoretical Framework

This article is anchored in two complementary theories. Risk Management Theory (RMT), developed by scholars such as Aven (2016), provides a structured, stepwise process for identifying, evaluating, and prioritising cyber risks, enabling targeted resource allocation aligned with threat severity and likelihood. In the Nigerian context, RMT is evident in the CBN's deployment of Biometric Verification Numbers (BVN) as a systemic vulnerability control mechanism (CBN, 2022). However, RMT's focus on quantifiable risks may undervalue qualitative elements such as organisational culture (Houghton & Smith, 2021), and static assessment models are less effective against rapidly evolving threats like AI-enhanced phishing (Chuang et al., 2022).

Systems Theory (ST), originating with Von Bertalanffy (1968), addresses these limitations by viewing cybersecurity as an emergent property of systemic interactions among technology, human behaviour, and organisational processes. Its emphasis on interdependence and feedback loops is central to understanding how vulnerabilities arise not from isolated failures but from complex interactions, such as poor interdepartmental communication combined with legacy systems. When applied together, RMT and ST provide a dual analytical advantage: RMT enables precise risk prioritisation while ST contextualises threats within their wider systemic and sociotechnical ecosystem.

III. METHODOLOGY

3.1 Research Design and Population

This article adopted a cross-sectional research design, which is well-suited to examining the prevalence, patterns, and relationships among variables at a specific point in time without manipulating the study context (Creswell, 2014; Levin, 2006). The target

population comprised bank employees, including IT security officers, risk management staff, compliance officers, and operations personnel, and customers of Tier-1 commercial banks (FUGAZ) headquartered in Lagos State, Nigeria's financial hub. Lagos State was selected as the study site given its centrality to Nigeria's financial operations and its concentration of high-volume digital transactions (Adelekan, 2020).

3.2 Sampling and Data Collection

Sample size was determined using Cochran's formula ($n = Z^2p(1-p)/E^2$) at a 95% confidence level ($Z = 1.96$), estimated proportion of 0.5, and 5% margin of error, yielding a minimum sample of 385 respondents. An additional 20% buffer was applied to account for non-responses, resulting in a target sample of 460 respondents, 230 bank staff and 230 customers. Simple random sampling was employed for both groups to ensure equal selection probability and eliminate bias (Etikan & Bala, 2017). Data were collected via structured self-administered questionnaires distributed through both physical and electronic channels to maximise accessibility and response rates (Sue & Ritter, 2012). Informed consent was obtained from all participants, and ethical approval was secured from the university's research board.

3.3 Research Instrument

The questionnaire was organised into four thematic sections addressing: (a) current cybersecurity threats, (b) implications of cyberattacks on bank operations and human security, (c) strategic responses, and (d) implementation challenges. Items employed a five-point Likert scale ranging from 'Strongly Disagree' (1) to 'Strongly Agree' (5). Content validity was established through expert review by cybersecurity and banking professionals, and a pilot test was conducted with a select group of Lagos-based bank staff to assess clarity and relevance (Polit & Beck, 2012). Internal reliability was confirmed using Cronbach's alpha coefficients exceeding the acceptable threshold of 0.70 (Tavakol & Dennick, 2011) for all constructs.

3.4 Data Analysis

Data analysis employed a combination of descriptive and inferential statistical techniques using SPSS software (Field, 2018). Descriptive statistics, means, standard deviations, frequencies, and percentages, summarised respondent profiles and perceptions. Pearson correlation analysis examined the directionality and strength of relationships among key constructs. Multiple regression analysis explored the predictive relationships between cybersecurity threat levels, strategic responses, and their implications. One-way Analysis of Variance (ANOVA) tested for significant perceptual differences based on staff specialisation. Qualitative open-ended responses were analysed using thematic analysis to surface emergent patterns regarding implementation challenges and stakeholder recommendations.

IV. RESULTS

4.1 Demographic Profile of Respondents

The investigation achieved a full response from all 460 targeted participants. Among bank staff (n = 230), the largest age cohort was 25–34 years (33.9%), indicating a relatively young, digitally familiar workforce, complemented by substantial representation from staff with over 10 years of experience (22.6%). The majority held a Bachelor's degree (39.6%) or Higher National Diploma (32.6%). Respondents were drawn from Risk Management (23.5%), Operations Management (20.4%), Information Technology (17.4%), Cybersecurity (14.8%), and other departments (23.9%), ensuring a comprehensive cross-functional perspective. Among customers (n = 230), 68.7% were aged 18–34, with a near-equal gender split. Notably, 76.1% had maintained their banking relationship for over four years, and 50.4% were primary users of mobile banking platforms, confirming the sample's deep engagement with the digital banking ecosystem. This demographic composition lends credibility and representativeness to the study's empirical findings.

4.2 Current Cybersecurity Threats Facing Nigerian Banks

The descriptive analysis of cybersecurity threat perceptions reveals a sector under persistent and multifaceted assault. The expansion of mobile banking was identified as the primary catalyst for increased vulnerability ($M = 3.62$, $SD = 1.115$), consistent with the finding of Sitorus et al. (2024) that 51% of mobile banking users have experienced cybercrime attempts. The view that cybercriminals continuously upgrade their tactics was strongly endorsed ($M = 3.58$, $SD = 1.137$), underscoring the dynamic, adaptive nature of the threat environment. Insider threats were rated as a major concern ($M = 3.59$, $SD = 1.128$), implicating employees as a critical

vulnerability through negligence, inadequate training, or malicious intent, a finding corroborating Ololade et al.'s (2020) identification of job insecurity and performance pressure as drivers of internal fraud. Frequent occurrence of phishing, ransomware, and malware was confirmed (M = 3.54, SD =1.087), as was the prevalence of DDoS attacks disrupting operations (M = 3.57, SD = 1.117). Social engineering was also identified as a common attack vector (M = 3.44, SD = 1.125), reinforcing the human element as the weakest link in the security chain (Siponen & Vance, 2010). Moderately rated were perceptions that customers feel unsafe (M = 3.04) and that banks lack adequate infrastructure (M = 3.03), suggesting a possible gap between the technical reality of threats and customer awareness, or a degree of trust-based risk acceptance.

4.3 Implications for Bank Operations and Human Security

The findings unequivocally demonstrate that cyberattacks impose severe, multifaceted consequences on both institutional operations and individual human security. The most prominent finding was the immense psychological and operational pressure placed on bank employees to protect customer financial stability (M = 4.02, SD = 0.803), the highest rated item in the study. This burden represents a significant human cost within the institutions themselves, potentially creating a vicious cycle of burnout-induced errors that further compromise security.

Service disruptions were identified as a major operational consequence (M = 3.57, SD = 1.128), directly compromising the reliability of banking, a foundational requirement of financial system stability. Data breaches compromising customer financial information (M = 3.55, SD = 1.100) and direct financial losses to banks and customers (M = 3.52, SD = 1.140) represent immediate human security violations. The human security impact deepens through the erosion of customer trust in digital platforms (M = 3.60, SD = 1.141) and heightened personal insecurity about using online services (M = 3.59, SD = 1.116). These findings operationalise the human security construct empirically: the fear generated by cyber incidents constitutes a tangible threat to 'freedom from fear,' while financial losses directly undermine economic security (UNDP, 1994; Daraojimba et al., 2023).

Critically, the disruption of essential financial services for vulnerable customers (M = 3.59, SD = 1.082) introduces a pronounced social equity dimension: pension payments, welfare transfers, and small-business liquidity can be severed by a single cyber incident, disproportionately affecting the most marginalised. Respondents further recognised that cyberattacks threaten national economic stability (M = 3.51) and can trigger broader socio-economic disruptions (M = 3.58), framing cybersecurity as a macro-prudential concern of the highest order.

4.4 Strategic Responses and Their Effectiveness

The evaluation of strategic responses reveals a landscape of commendable progress in foundational areas but marked by critical deficiencies in advanced and collaborative domains. Multi-factor authentication (MFA) was the most strongly endorsed measure (M = 4.05, SD = 0.825), followed by regular security audits (M = 4.01, SD = 0.819), reflecting successful institutionalisation of regulatory-driven best practices aligned with the CBN's (2018) Risk-Based Cybersecurity Framework. Compliance with international standards such as PCI DSS (M = 3.60) and regular system upgrades (M = 3.58) were also positively rated.

However, critical gaps were identified. Encryption technology implementation received one of the lowest mean scores (M = 3.17, SD = 1.489), with high standard deviation indicating significant inconsistency across institutions. Most alarmingly, collaboration with cybersecurity firms and government agencies received the lowest rating of all strategic measures (M = 3.12, SD = 1.396), indicating strategic isolation that prevents effective threat intelligence sharing and coordinated response, the very mechanisms most valued in developed-economy models (Gao et al., 2021). The effectiveness of incident response plans (M = 3.19) and sufficiency of anti-phishing measures (M = 3.46) also suggest concerning gaps in response preparedness.

A defining finding of this study is what is termed the 'Effectiveness Paradox.' While customers reported feeling significantly more secure using digital banking compared to previous years (M = 4.09, SD = 0.803) and agreed that measures have improved overall confidence (M = 4.00, SD = 0.793), they simultaneously expressed near-neutral agreement that strategic responses have reduced successful attacks (M = 2.97, SD = 1.333) or data breach risks

(M = 2.99, SD = 1.417). This dissonance indicates that banks have succeeded in creating a perception of security, vital for digital adoption, while falling short of tangibly reducing the actual threat incidence. Effectiveness against insider threats was particularly low (M = 3.05), corroborating identified deficiencies in internal controls and monitoring.

4.5 Implementation Challenges: The Expertise Paradox and Inferential Analysis

ANOVA revealed statistically significant perceptual differences based on staff specialisation ($p < .05$). Risk Management and IT/Cybersecurity professionals expressed significantly lower confidence in the effectiveness of strategic responses compared to colleagues in Operations Management. This internal 'expertise paradox' constitutes a critical governance failure: the individuals with the deepest technical understanding of vulnerabilities, the experts tasked with managing risk, are the least confident in the organisation's defensive posture. This internal disconnect likely stems from divergent success metrics and echoes the warnings of Von Solms and Van Niekerk (2013) regarding the dangers of organisational silos in cybersecurity governance.

The regression analysis revealed low explanatory power ($R^2 = 9.5\%$ in the multiple regression model), demonstrating that the mere presence of threats and implemented responses accounts for very little of the actual negative outcomes experienced. This powerfully affirms the Systems Theory framework: cybersecurity resilience is an emergent property of complex socio-technical interactions, including organisational culture, leadership commitment, vendor management, and national infrastructure, rather than a simple product of deployed technical controls (Checkland, 1999; Hirschheim & Klein, 2012). Qualitative responses provided stakeholder-articulated clarity, calling consistently for 'stricter regulatory enforcement,' 'national threat intelligence sharing,' and 'continuous, sophisticated staff training.' These recurring themes confirm that the primary barrier is not a knowledge gap but an implementation gap driven by resource constraints, regulatory inertia, and insufficient collaborative will.

V. DISCUSSION

The findings of this study advance the discourse on banking cybersecurity in three significant dimensions. First, they provide robust empirical validation for the human security framing of cybersecurity threats, a perspective theorised in the literature but rarely operationalised with primary data from a sub-Saharan African context. The data confirm that cyberattacks constitute a comprehensive threat to human security, eroding economic stability, generating personal fear, and disrupting essential services for vulnerable populations in ways that align directly with the seven pillars articulated by UNDP (1994). This reframes cybersecurity investment from a corporate IT expense to a simultaneous investment in operational continuity, financial integrity, customer retention, employee well-being, and national economic resilience.

Second, the identification of the 'Effectiveness Paradox' challenges a dominant assumption in compliance-oriented cybersecurity literature and practice: that implementing a framework of controls is synonymous with effectively mitigating risk. The divergence between elevated perceived personal security and neutral assessments of actual threat reduction suggests an overinvestment in customer-facing deterrents (particularly MFA) at the expense of less visible but more operationally critical investments in advanced threat detection, network segmentation, and proactive threat hunting. This finding has direct implications for how regulators and institutions assess security effectiveness, arguing forcefully for a shift from activity-based to outcome-based evaluation metrics.

Third, the 'expertise paradox' identified via ANOVA represents a novel theoretical contribution to the application of Systems Theory in cybersecurity governance. By demonstrating that intra-organisational perceptual divergence between technical experts and operational staff can fundamentally undermine resilience, the study extends the literature on cybersecurity culture (Von Solms & Van Niekerk, 2013; Siponen & Vance, 2010) into the domain of internal governance. It challenges the assumption of organisational unity in risk perception and suggests that internal communication frameworks and governance structures are as determinative of security outcomes as any technological control. The low R-squared values from the regression analysis provide statistical corroboration for this systemic interpretation, consistent with the warnings of scholars who caution against linear, checklist-based models of security effectiveness (Anderson & Moore, 2007).

© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716597

Comparatively, Nigeria's cybersecurity trajectory mirrors the experience of other emerging economies such as Brazil and India, where rapid digitalisation has outpaced regulatory capacity and institutional readiness (Santos, 2021; Singh, 2021). However, Nigeria's specific combination of cashless economy policy-driven digital acceleration, widespread mobile-first banking adoption on potentially insecure devices, and a youthful but inadequately trained cybersecurity workforce creates a distinctive and acute risk profile. The lessons from developed-economy models, mandatory threat intelligence sharing (CISA, 2015), continuous risk assessment (FSA Japan, 2018), and capacity-building frameworks, offer actionable pathways for Nigerian policymakers, but must be adapted to the resource and infrastructural constraints of the Nigerian context.

VI. CONCLUSION AND RECOMMENDATIONS

6.1 Conclusion

This study interrogates the interplay between cybersecurity threats, banking stability, and human security in Nigeria's rapidly digitalising financial sector. The evidence conclusively establishes that Nigerian banks are entrenched in a high-threat environment where technological adoption, particularly mobile banking, has outpaced the maturation of corresponding security cultures and infrastructures. The sector has commendably established foundational cyber hygiene, evidenced by high MFA and security audit adoption, but this foundation is insufficient against contemporary threats. The documented 'Effectiveness Paradox' and internal 'expertise paradox' are symptomatic of a broader systemic failure to transition from reactive, compliance-based security to proactive, intelligence-led, and collaboratively-oriented resilience.

The investigation provides irrefutable empirical evidence that cybersecurity failures have direct and deleterious consequences for human security, eroding trust, exacerbating personal insecurity, and disrupting essential services, thereby actively undermining individual and community well-being. Cybersecurity is thus repositioned from a corporate IT concern to a national imperative at the intersection of economic policy, social protection, and national security. The evidence clearly indicates that securing Nigeria's digital financial infrastructure is essential not only for banking stability but for the realisation of broader developmental goals, including financial inclusion and sustainable digital transformation.

6.2 Recommendations

For Nigerian Banks Banks should escalate cybersecurity investment from a defensive to a pre-emptive posture by establishing dedicated Security Operations Centres powered by AI and machine learning for predictive threat analytics. The adoption of a Zero Trust security architecture is essential to address insider threats and data vulnerabilities through strict access controls, network segmentation, and end-to-end data encryption. Internal governance must be reformed by instituting cross-functional cybersecurity committees with real decision-making authority, and by linking departmental Key Performance Indicators to specific security outcomes, ensuring expert risk assessments directly inform strategic resource allocation.

For Regulatory Bodies (Central Bank of Nigeria)

The CBN must evolve its oversight from periodic auditing to continuous, risk-based monitoring with graduated material financial penalties for non-compliance and incident nondisclosure. Most critically, the CBN should formally establish, resource, and mandate participation in a sector-wide Computer Emergency Response Team with the authority to aggregate, analyse, and disseminate actionable threat intelligence to all licensed financial entities in real time. Legal frameworks must protect shared intelligence while mandating participation from banks, telecommunications providers, and FinTech firms, creating an integrated national defence network.

For Government and Public Policy

A dual-track national capacity-building programme is required. The first track should deliver a sustained, multi-channel public education campaign, deployed through media, educational institutions, and community networks, to raise the digital hygiene of the citizenry, treating public cybersecurity awareness as a public good. The second track must address the severe cybersecurity talent shortage by funding partnerships between academia and industry to develop specialised curricula, certifications, and apprenticeship programmes, building a sustainable pipeline of indigenous expertise to defend national digital assets.

DECLARATIONS

Ethical approval was obtained from the relevant university research board. Informed consent was secured from all participants prior to data collection. This study received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors. The author declares no conflict of interest.

REFERENCES

[1] Adegbite, A. O., Akinwolemiwa, D. I., Uwaoma, P. U., Kaggwa, S., Akindote, O. J., & Dawodu,

[2] S. O. (2023). Review of cybersecurity strategies in protecting bank infrastructure: Perspectives from the USA. Computer Science & IT Research Journal, 4(3), 200–219. https://doi.org/10.51594/csitrj.v4i3.658

[3] Adelekan, I. (2020). Lagos: A critical driver of Nigeria's economy. Lagos Business School Review.

[4] Adeniyi, J. (2024). Nigerian banks hit by cyberattacks: Hope Payment Service Bank loses N10 billion. BusinessDay. https://businessday.ng

[5] Agwulonu, C., & Ijaseun, T. (2024). Phishing attacks and bank customer authentication in Nigeria. Journal of Cybersecurity Research, 6(1), 12–28.

[6] Ajufo, G., & Qutieshat, A. (2023). An examination of the human factors in cybersecurity: Future direction for Nigerian banks. Indonesian Journal of Information Systems, 6(1), 1–16.

[7] Anderson, R., & Moore, T. (2007). The economics of information security. Science, 314(5799), 610–613.

[8] Aven, T. (2016). Risk analysis: Assessing uncertainties beyond expected values and probabilities. John Wiley & Sons.

[9] Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber resilience—fundamentals for a definition. Proceedings of the 8th International Conference on Availability, Reliability, and Security, 35–43.

[10] Brower, D., & McCormick, J. (2021). The Colonial Pipeline ransomware attack: Lessons for future cyber defence. Journal of Security Studies, 16(3), 204–210.

[11] Central Bank of Nigeria. (2018). Risk-based cybersecurity framework and guidelines for deposit money banks and payment service providers. CBN. https://www.cbn.gov.ng

[12] Central Bank of Nigeria. (2019). Guidelines on information security management for banks and other financial institutions. CBN.

[13] Central Bank of Nigeria. (2020). Payment systems vision 2025. CBN.

[14] Central Bank of Nigeria. (2022). Annual report on cybercrime and cybersecurity. CBN.

[15] Checkland, P. (1999). Systems thinking, systems practice. John Wiley & Sons.

[16] Chen, S., Fan, L., Meng, G., Su, T., Xue, M., Xue, Y., & Xu, L. (2020). An empirical assessment of security risks of global android banking apps. Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering, 1310–1322.

[17] Chuang, T., Chang, S., & Huang, C. (2022). Cybersecurity risk management in banking: A framework and empirical validation. International Journal of Information Management, 63, 102–116.

[18] Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods approaches (4th ed.). SAGE Publications.

[19] Dandurand, L., & Serrano, O. S. (2013). Towards improved cyber security information sharing.

[20] Proceedings of the 5th International Conference on Cyber Conflict, 2(1), 37–50.

[21] Daraojimba, C., Onunka, O., Alabi, A. M., Okafor, C. M., Obiki-Osafiele, A. N., & Onunka, T. (2023). Cybersecurity in US and Nigeria banking and financial institutions: Review and assessing risks and economic impacts. Acta Informatica Malaysia, 7(1), 54–62.

[22] Eling, M., & Schnell, W. (2016). Hacking events, the number of data records affected, and the economic impact of cybercrime. Journal of Risk and Insurance, 83(3), 475–500.

[23] Etikan, I., & Bala, K. (2017). Sampling and sampling methods. Biometrics & Biostatistics International Journal, 5(6), 215–217.

[24] Fadare, O., Odukoya, E., & Olatunji, S. (2023). Digital adoption, cybercrime, and the enforcement gap in Nigeria's post-pandemic banking sector. African Journal of Cybersecurity, 11(2), 44–61.

[25] Familoni, B. T., & Shoetan, P. O. (2024). Cybersecurity in the financial sector: A comparative analysis of the USA and Nigeria.

Computer Science & IT Research Journal, 5(4), 850–877.

[26] Federal Republic of Nigeria. (2015). Cybercrimes (Prohibition, Prevention, etc.) Act. Government Press.

[27] Field, A. (2018). Discovering statistics using IBM SPSS statistics (5th ed.). SAGE Publications.

[28] Gao, Z., Xu, J., & Li, Y. (2021). Challenges in cybersecurity compliance in developing economies.

[29] Journal of Information Technology Management, 33(4), 203–215.

[30] Hassan, A. O., Ewuga, S. K., Abdul, A. A., Abrahams, T. O., Oladeinde, M., & Dawodu, S. O.

[31] (2024). Cybersecurity in banking: A global perspective with a focus on Nigerian practices. Computer Science & IT Research Journal, 5(1), 41–59.

[32] Hirschheim, R., & Klein, H. (2012). Balancing security and productivity in organisations. Journal of Information Security, 8(4), 304–316.

[33] Hoffman, D., Wills, T., & Pereira, J. (2020). Systemic weaknesses in cybersecurity governance. Journal of Cybersecurity Policy, 4(1), 55–74.

[34] Houghton, L., & Smith, A. (2021). The systems perspective on cybersecurity: Developing a unified approach. Computers & Security, 104, 102–114.

[35] IBM Security. (2023). Cost of a data breach report 2023. IBM.

[36] https://www.ibm.com/security/data-breach

[37] Inkster, B., Knibbs, C., & Bada, M. (2023). Cybersecurity: A critical priority for digital mental health. Frontiers in Digital Health, 5, 1242264. https://doi.org/10.3389/fdgth.2023.1242264

[38] Interpol. (2022). Ransomware: Global threat report. Interpol.

[39] Japan's Ministry of Economy, Trade and Industry. (2018). Basic Act on Cybersecurity. Government of Japan.

[40] Kaspersen, A., & Lindsey, N. (2014). Cybercrime and human security: Emerging threats in the digital economy. International Security Review, 18(3), 78–94.

[41] Kaspersky Lab. (2015). The great bank robbery: Carbanak APT. Kaspersky Lab.

[42] Kim, S. (2022). The Lazarus Group and North Korea's global cybercriminal activities. Cybersecurity Journal, 5(2), 45–58.

[43] Koops, B.-J., & Leenes, R. (2014). Privacy regulation in the EU and global influence of GDPR. Computer Law & Security Review, 30(5), 487–497.

[44] Kovács, K., & Spalek, S. (2016). Cyber threats and the erosion of human security: Evidence from financial systems. European Journal of Security Studies, 9(2), 112–130.

[45] Levin, K. A. (2006). Study design III: Cross-sectional studies. Evidence-Based Dentistry, 7(1), 24–25.

[46] Lottu, O. A., Abdul, A. A., Daraojimba, D. O., Alabi, A. M., John-Ladega, A. A., & Daraojimba, C. (2023). Digital transformation in banking: A review of Nigeria's journey to economic prosperity. International Journal of Advanced Economics, 5(8), 215–238.

[47] Mahbub ul Haq, M. (1995). Reflections on human development. Oxford University Press.

[48] Maleks Smith, K., Brown, P. M., & Evans, A. G. (2020). The global economic impact of cybercrime. Economic Perspectives, 64(2), 34–46.

[49] Matsuura, J. (2016). Strategic responses to cybersecurity: An integrated framework. International Journal of Digital Security, 3(1), 77–92.

[50] Natalucci, F., Qureshi, M. S., & Suntheim, F. (2024, April 9). Rising cyber threats pose serious concerns for financial stability. International Monetary Fund. https://www.imf.org/en/Blogs/Articles/2024/04/09

[51] National Information Technology Development Agency. (2019). Nigeria Data Protection Regulation (NDPR). NITDA.

[52] NeFF. (2024). Nigeria Electronic Fraud Forum annual report 2023. CBN.

[53] Nigerian Communications Commission. (2023). State of cybersecurity in Nigeria. NCC.

[54] Nosrati, L., & Bidgoli, A. M. (2016). A review of mobile banking security. 2016 IEEE Canadian Conference on Electrical and Computer Engineering, 1–5.

[55] Obi, O. C., Akagha, O. V., Dawodu, S. O., Anyanwu, A. C., Onwusinkwue, S., & Ahmad, I. A. I. (2024). Comprehensive review on cybersecurity: Modern threats and advanced

defence strategies. Computer Science & IT Research Journal, 5(2), 293–310.

[56] Ololade, B. M., Salawu, M. K., & Adekanmi, A. D. (2020). E-fraud in Nigerian banks: Why and how? Journal of Financial Risk Management, 9(3), 211–228.

[57] Olukoya, J. (2022). Cybersecurity compliance and resilience in Nigerian banks: Regulatory gaps and challenges. Journal of Banking Regulation, 10(2), 140–158.

[58] Onyekachi, E. (2024). Cybersecurity skills gap in Nigerian banking sector. African Journal of Information Technology, 19(1), 45–52.

[59] Oyewole, A. T., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies application. World Journal of Advanced Research and Reviews, 21(3), 625–643.

[60] Polit, D. F., & Beck, C. T. (2012). Nursing research: Generating and assessing evidence for nursing practice (9th ed.). Lippincott Williams & Wilkins.

[61] 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.

[62] Ruan, K., Carthy, J., Kechadi, T., & Baggili, I. (2019). Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results. Digital Investigation, 10(1), 34–43.

[63] Santos, L. (2021). Public-private partnerships and cybersecurity in Brazil. Brazilian Journal of Public Policy, 17(2), 110–123.

[64] Sarumi, J., & Omotosho, O. M. (2022). A review of network security strategies employed by the Nigerian banking sector: Case study of Access Bank PLC, Bariga, Lagos, Nigeria. Advances in Multidisciplinary and Scientific Research Journal Publication, 8, 1–10.

[65] Singh, A. (2021). Cybersecurity risks and regulatory frameworks in India. South Asian Cybersecurity Review, 8(3), 23–34.

[66] Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. MIS Quarterly, 34(3), 487–502.

[67] Sitorus, R. S., Hutagaol, B. J., & Simanjuntak, D. M. (2024). Capability-based API gateway technology selection analysis for banking cybersecurity solution using AHP method. Sinkron: Jurnal dan Penelitian Teknik Informatika, 9(1), 338–347.

[68] Sue, V. M., & Ritter, L. A. (2012). Conducting online surveys (2nd ed.). SAGE Publications.

[69] Takemura, M. (2022). Information-sharing challenges in Japan's cybersecurity framework. Journal of Information Technology and Policy, 19(1), 13–26.

[70] Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. International Journal of Medical Education, 2, 53–55.

[71] United Nations Development Programme. (1994). Human development report 1994: New dimensions of human security. UNDP.

[72] Von Bertalanffy, L. (1968). General system theory: Foundations, development, applications. George Braziller.

[73] Von Solms, R., & Van Niekerk, J. (2013). From information security to cybersecurity. Computers & Security, 38(2), 97–102.

[74] Wang, V., Nnaji, H., & Jung, J. (2020). Internet banking in Nigeria: Cyber security breaches, practices and capability. International Journal of Law, Crime and Justice, 62, 100415.

[75] Williams, R. (2017). The future of cybersecurity in financial services. Journal of Financial Services Technology, 14(4), 29–42.

[76] World Economic Forum. (2022). Global risks report 2022. WEF.

[77] World Economic Forum. (2023). Global risks report 2023. WEF.

[78] Wu, Y., Cheng, X., & Zhang, Y. (2023). Bank cybersecurity crisis management: International experience, analytical framework and path selection. Sage Publications, 11(2222-1735). https://doi.org/10.1145/3625469.3625487