https://doi.org/10.65025/ICAIC25115o

Strengthening Cybersecurity in Nigeria's Remote Financial Workspaces: Bridging Policy and Practice

Adoikwu Pius Odeh
International Organization for Migration, Nigeria.
piusodeh@gmail.com

Acheme Okolobia Odeh
Bahcesehir Cyprus University, Cyprus
odehoklobia@gmail.com

Abstract
This study investigates the challenges of maintaining cybersecurity standards in remote work within Nigerian financial institutions after the COVID-19 pandemic. It examines the effectiveness of regulatory frameworks, institutional practices, and the adoption of cybersecurity strategies, addressing four research questions through peer-reviewed literature, regulatory documents, and industry reports. The findings reveal that Nigerian financial institutions face persistent threats such as phishing, ransomware, and credential theft, which surged during the pandemic. Although basic measures like multi-factor authentication and VPNs are common, adoption of advanced tools such as zero-trust architecture remains limited. Regulatory frameworks, including the CBN's Risk-Based Cybersecurity Framework and the NDPR, provide important baselines but are often rigid and unevenly enforced, particularly among smaller institutions. Tier-1 banks demonstrate stronger compliance, but systemic capacity gaps remain across the sector. The study concludes that while progress has been made, institutions remain largely reactive rather than proactive, leaving them vulnerable to evolving risks. It recommends enhancing regulatory adaptability, strengthening institutional capacity, fostering intelligence sharing, and accelerating adoption of advanced cybersecurity measures. These steps would enable Nigerian financial institutions to shift from compliance-driven responses to proactive resilience strategies, aligning with global best practices and safeguarding their operations in an increasingly digital world.

Keywords
Cybersecurity, Remote Work, Nigerian Financial Institutions, Regulatory Frameworks, Post-COVID-19.

Introduction

1.1. Background of the Study, Research Problem, and Significance

The COVID-19 pandemic triggered a global shift toward remote work, a transformation that brought major cybersecurity implications, especially for Nigeria's financial sector. While remote work enabled operational continuity during lockdowns, it also expanded cyber vulnerabilities, many institutions deployed access tools hastily, often lacking proper safeguards (Brynjolfsson et al., 2020; Chamola et al., 2020). In Nigeria, these challenges were compounded by outdated infrastructure, limited IT capacity, and weak enforcement of data protection policies (Reis et al., 2024; Familoni and Shoetan, 2024; ThisDayLive, 2023).

Although regulatory instruments such as the Nigeria Data Protection Regulation (NDPR) and the Central Bank of Nigeria (CBN)'s Risk-Based Cybersecurity Framework were introduced, implementation remains inconsistent and misaligned with global standards like the General Data Protection Regulation (GDPR) (CBN, 2021; NDPR, 2019; ITU, 2021). As a result, Nigerian financial institutions continue to face increasing cyberattacks, with enforcement and compliance falling behind the pace of technological change (Adedeji, 2025; Gbenga Femi et al., 2025).

This study, titled Challenges in Maintaining Cybersecurity Standards in Remote Work in Nigerian Financial Institutions Post-COVID-19: An Analysis of Regulatory Frameworks and Industry Practices, addresses a critical research gap: the disconnect between policy and real-world cybersecurity practice in remote work settings. While existing literature explores general cybersecurity risks in remote environments (Chamola et al., 2020; Brynjolfsson et al., 2020), limited attention has been given to Nigeria's unique context. Studies by Reis et al. (2024) and Familoni and Shoetan (2024) highlight this gap, noting discrepancies between regulatory intent and actual outcomes in Nigerian banks.

This research therefore investigates how well Nigerian financial institutions and regulators have adapted to the demands of cybersecurity in remote work settings. It critically examines the challenges these institutions face, evaluates the effectiveness of existing regulatory measures, and identifies opportunities for strengthening cybersecurity resilience in the post-pandemic digital economy.

The significance of this research lies in its dual contribution. Theoretically, it deepens understanding of cybersecurity governance in emerging markets during crisis-driven digital transitions. Practically, it provides actionable, context-specific recommendations to help institutions strengthen cybersecurity measures and better align with global standards. Financial institutions are not only stewards of sensitive data but also central to economic stability, enhancing their digital resilience is therefore essential. By

bridging the gap between regulation and implementation, this study informs both scholarly dialogue and future policy reforms to protect Nigeria's financial ecosystem in a remote-first era.

1.2. Research Aim and Objectives

This study aims to examine the challenges Nigerian financial institutions face in maintaining cybersecurity standards in remote work environments following the COVID-19 pandemic. It further seeks to evaluate the effectiveness of existing regulatory frameworks and institutional practices in addressing these challenges, with the goal of offering evidence-based recommendations to strengthen cybersecurity resilience.

1.3. Research Objectives

2. To identify and analyze five key cybersecurity challenges associated with remote work in Nigerian financial institutions post-COVID-19.
3. To critically assess the effectiveness of at least three cybersecurity regulatory frameworks (2015–2024) in addressing remote work-related threats.
4. To evaluate at least three cybersecurity practices adopted by Nigerian financial institutions to secure remote work environments.
5. To develop evidence-based recommendations for enhancing cybersecurity resilience in remote work models within Nigeria's financial sector.

1.4. Research Questions

1. What are the key cybersecurity risks and systemic vulnerabilities Nigerian financial institutions face in managing remote work environments post-COVID-19?
2. To what extent do existing regulatory policies effectively address cybersecurity risks related to remote work?
3. What cybersecurity strategies have institutions implemented, and how effective are they?
4. What evidence-based recommendations can improve the cybersecurity resilience of financial institutions operating remotely in the post-pandemic era?

2. Literature Review

2.1. Introduction

The COVID-19 pandemic forced a global shift to remote work, ensuring business continuity but exposing organizations to new cybersecurity risks. Nigeria's financial institutions were particularly vulnerable, as over 60% of developing countries, including Nigeria, lacked frameworks designed for remote operations (ITU, 2021; NCC, 2022). During this period, cyber incidents in the sector rose by 31%. While global standards such as NIST and the UK's FCA offer strong guidance, their adoption in Nigeria remains limited (Nurse et al., 2021; Oyeniyi et al., 2024). This review examines these challenges, focusing on regulatory and institutional responses rather than technical solutions.

2.2. Conceptual Review (Study Variables)

2.2.1. Cybersecurity Standards

Cybersecurity standards are structured sets of guidelines designed to secure digital systems and protect sensitive information. Globally, frameworks such as ISO/IEC 27001:2013 and the NIST Cybersecurity Framework establish consistent protocols for risk management, incident detection, and resilience (ISO, 2013; NIST, 2018). Within financial services, compliance with such standards is critical to safeguard customer data, ensure operational continuity, and maintain trust.

In Nigeria, the Central Bank of Nigeria (CBN, 2021) and the Nigeria Data Protection Regulation (NDPR, 2019) have developed frameworks tailored to banking institutions. However, despite the presence of these regulations, enforcement remains inconsistent and often lags behind global best practices such as the European Union's General Data Protection Regulation (GDPR). Nigeria was ranked 47th globally in the Global Cybersecurity Index, reflecting gaps in translating policy into effective practice (ITU, 2021). These weaknesses reveal a need for more dynamic frameworks capable of addressing emerging risks associated with remote working models.

2.2.2. Remote Work Practices

Remote work, defined as the decentralization of work away from traditional office environments, became the dominant mode of operation during the COVID-19 pandemic. While this ensured continuity, it also expanded the digital "attack surface" of organizations. Employees working from home often relied on unsecured personal devices, weakly protected networks, and cloud-based services, exposing financial institutions to heightened risks of ransomware, phishing, and credential theft (Brynjolfsson et al., 2020; Chamola et al., 2020).

Many Banks in Nigeria lacked robust virtual private network (VPN) infrastructure and failed to implement consistent multi-factor authentication (MFA) or cyber hygiene training, leaving them highly vulnerable (Akinsanya and Akande, 2021). These gaps highlight how remote work environments introduced novel security challenges that were inadequately anticipated by existing standards and regulatory frameworks.

2.2.3. Regulatory Frameworks

Regulation serves as the foundation for cybersecurity governance, ensuring that institutions adhere to minimum standards of data protection and operational security. The CBN's Risk-Based Cybersecurity Framework (2021) mandated banks to conduct regular risk assessments, incident reporting, and adopt layered security controls. Similarly, the NDPR emphasized personal data protection and compliance with privacy principles (NDPR, 2019).

Despite these measures, smaller banks often lack the technical capacity and human resources to meet compliance requirements (Edeh and Eze, 2021). Moreover, regulatory enforcement in Nigeria tends to be reactive rather than proactive, limiting its effectiveness in addressing dynamic cyber risks (Carnegie Endowment for International Peace, 2022). When you compare this with international standards such as NIST and ISO/IEC 27001, Nigerian regulations remain prescriptive and less adaptable, creating implementation gaps in a rapidly evolving threat landscape.

2.2.4. Industry Practices

Nigerian financial institutions have responded to cybersecurity risks through diverse organizational practices, though capacity differs significantly across institutions. Larger Banks have invested in endpoint protection, remote access controls, and awareness training campaigns, including initiatives such as the Moni Sense programme and FirstBank's cybersecurity webinars (Okoye, Chidiebere and Ogunleye, 2021; Verizon, 2022). These efforts reflect an increasing recognition of the human factor in cyber resilience, as social engineering remains a dominant threat vector globally.

However, smaller institutions still face challenges in adopting advanced practices such as zero-trust architectures and artificial intelligence-driven monitoring, which are common in international Banks (Panchal, 2020; Chin, 2022). This fragmentation underscores the uneven maturity of industry practices within Nigeria's financial sector.

2.3. Theoretical Framework

This study is anchored on two interrelated theories - the Cybersecurity Maturity Model (CMM) and Regulatory Compliance Theory. These, together provide a balanced lens for evaluating how Nigerian financial institutions manage cybersecurity risks in the era of remote work.

The CMM assesses institutional readiness by categorizing cybersecurity practices into maturity levels ranging from initial ad hoc measures to optimized, adaptive strategies (Caralli, Knight and Montgomery, 2012; U.S. Department of Energy, 2022). This framework helps organizations identify weaknesses, prioritize improvements, and benchmark progress against global standards. While widely applied across industries, scholars caution that maturity models risk becoming static and less effective in dynamic threat environments unless regularly adapted (Rabii et al., 2020; Büyüközkan and Güler, 2025). In the Nigerian context, where financial institutions face resource and infrastructure constraints, tailoring maturity models to local realities is critical.

Complementing this is the Regulatory Compliance Theory which explains why organizations adopt or resist regulatory requirements, emphasizing the role of internal culture, legitimacy, and enforcement mechanisms (Ayres and Braithwaite, 1992; Parker and Nielsen, 2011). In Nigeria, limited enforcement capacity means voluntary compliance and organizational culture play a pivotal role in shaping cybersecurity outcomes. Taken together, these theories allow a multidimensional assessment of both technical and behavioral readiness within Nigerian Banks.

2.4. Relationships Between Variables

The relationship between cybersecurity standards, remote work practices, regulatory frameworks, and industry responses is highly interdependent. Remote work, while essential during the COVID-19 pandemic, expanded organizational exposure by shifting activities into insecure environments. The reliance on personal devices and home networks created vulnerabilities that existing standards, designed for centralized systems were not fully equipped to address (Brynjolfsson et al., 2020; Ferreira and Cruz-Cunha, 2020). Nigerian banks that failed to adopt multi-factor authentication or endpoint security reported higher risks, underscoring the inadequacy of conventional safeguards in remote contexts (Akinsanya and Akande, 2021).

Regulatory frameworks such as the CBN's Risk-Based Cybersecurity Framework were intended to mitigate these risks through mandatory assessments and layered controls. However, compliance has been uneven, such that, larger banks with resources generally achieve maturity, while smaller institutions continue to struggle (CBN, 2021; Edeh and Eze, 2021). This disparity reveals a critical gap between policy intent and institutional capacity, where regulation exists in principle but not in consistent practice (Carnegie Endowment for International Peace, 2022).

Industry responses reflect this imbalance. Global firms have embraced zero-trust architectures and AI-driven monitoring (Panchal, 2020; Chin, 2022), whereas Nigerian banks demonstrate fragmented adoption, with Tier-1 institutions advancing while others lag (Okoye, Chidiebere and Ogunleye, 2021). Evidence from existing studies suggests that the strength of Nigeria's financial sector lies not in adopting regulations or technologies in isolation, but in how effectively regulatory frameworks, institutional capacity, and everyday security practices are integrated to address the evolving risks of remote work.

2.5. Empirical Review

Empirical studies on cybersecurity in Nigeria's financial sector reveal a fragmented but evolving landscape. Abubakar, Yusuf and Olayemi (2022) highlight that cyberattacks against Nigerian banks surged during COVID-19, with phishing and credential theft as dominant threats. Deloitte (2020) similarly reported that outdated infrastructure and limited budgets intensified vulnerability to socially engineered attacks. Empirical evidence also shows mixed levels of regulatory compliance, with Tier-1 banks achieving higher maturity compared to smaller institutions (Edeh and Eze, 2021). Awareness campaigns, such as Moni Sense and FirstBank's webinars, have improved staff cyber hygiene (Verizon, 2022). However, comparative studies stress that Nigeria still

lags international counterparts in adopting zero-trust architectures, AI-driven threat detection, and collaborative intelligence-sharing mechanisms (Chin, 2022; UK Finance, 2023).

2.6. Research Gap and Summary

The reviewed literature reveals that while Nigeria has developed regulatory frameworks and institutions have adopted various security measures, significant gaps persist. Few studies explicitly examine the intersection of remote work, regulatory compliance, and institutional maturity in Nigerian financial institutions post-COVID-19. Existing works are either overly technical or limited in scope, neglecting organizational and behavioral dimensions. This study therefore addresses a critical gap by integrating the Cybersecurity Maturity Model and Regulatory Compliance Theory to evaluate both structural and behavioral readiness within Nigeria's financial sector.

3. Research Methodology

3.1 . Research Approach and Design

This research adopts an interpretivist philosophy, which emphasizes the understanding of human experiences and institutional realities over the search for one objective truth. Given the focus on Nigerian financial institutions' responses to cybersecurity challenges within remote work environments, this approach is highly appropriate. Interpretivism allows the researcher to uncover the nuanced and context-specific ways institutions perceive, interpret, and implement cybersecurity measures (Saunders, Lewis and Thornhill, 2019).

From an ontological perspective, this study assumes that reality is socially constructed and varies between institutions, influenced by internal capacity, regulatory pressure, and technological maturity. Epistemologically, the research values subjective meaning over quantification, drawing insights from policy reports, academic literature, and industry documents (Scott, 1990). The axiological position accepts the researcher's influence in shaping the research focus and interpretation, particularly when assessing compliance trends and institutional behavior.

The chosen research design is qualitative and exploratory, using a secondary-data documentary analysis approach. This design is especially suitable because cybersecurity in Nigeria's financial sector is shaped by regulatory, institutional, and human factors that cannot be fully captured through numbers alone. In addition, financial institutions rarely disclose sensitive internal data, making the use of secondary data both practical and reliable. Rather than testing a hypothesis, the qualitative design emphasizes exploration and thematic analysis, enabling the study to generate context-specific insights that align with the applied nature of the research (Bryman, 2016).

Thus, the interpretivist, qualitative design is not only consistent with the research paradigm but also uniquely suited to address the cybersecurity challenges facing Nigerian financial institutions in the remote work era.

3.2. Research Sampling, Description and Sources of Secondary Data Selected

This study adopts a purposive sampling strategy, appropriate for qualitative research aimed at gaining rich, context-specific insights rather than statistical generalization (Palinkas et al., 2015). The selected secondary data sources are chosen based on their direct relevance to the themes of cybersecurity, remote work, and Nigeria's financial services sector in the post-COVID-19 context. This method supports interpretive inquiry by focusing only on sources that meaningfully contribute to understanding institutional behavior and regulatory responses.

The data set includes peer-reviewed journal articles, government and regulatory documents such as the CBN Risk-Based Cybersecurity Framework (CBN, 2021) as well as industry white papers, think tank publications, and media reports from reputable outlets like BusinessDay and Vanguard. This mix allows for methodological triangulation, enriching the study through multiple lenses (Saunders, Lewis and Thornhill, 2019). Sources span majorly from 2018 to 2024, capturing trends before and after the pandemic's digital disruption.

Academic sources were retrieved from scholarly databases like Google Scholar, ProQuest, while institutional data came from websites of the Central Bank of Nigeria, Nigerian Inter-Bank Settlement System (NIBSS), Nigerian Communications Commission (NCC), and cybersecurity-focused organizations such as KPMG and Deloitte Nigeria. Reports like NIBSS (2023), which revealed a 42% increase in attempted digital fraud in 2022, provide critical, real-world context for interpreting the secondary data. This carefully curated sampling enables the research to critically evaluate how Nigerian financial institutions have responded to cybersecurity threats within evolving remote work frameworks.

Accordingly, purposive sampling ensures that the sources selected are both contextually relevant and methodologically appropriate for achieving the objectives of this study.

3.3. Quality of Secondary Data

Ensuring the quality of secondary data is fundamental to maintaining the reliability and validity of this research. In line with Scott's (1990) framework, four criteria: authenticity, credibility, representativeness, and meaning, guided the evaluation, ensuring contextual relevance and academic soundness.

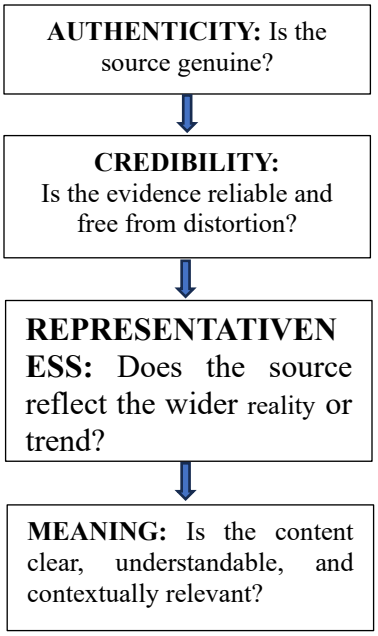

Figure 3.1: Four Key Criteria for Assessing Documentary Sources
Source: Adapted from Scott (1990).

Academic publications were selected only if they were peer-reviewed and published in internationally recognized journals, particularly those indexed in Google Scholar, and ProQuest. Studies from leading journals such as Computers and Security, Information and Computer Security, and Journal of Cybersecurity were prioritized. In addition, policy documents and reports from authoritative organizations like the Central Bank of Nigeria (CBN), the National Information Technology Development Agency (NITDA), the International Telecommunication Union (ITU), and International Organization for Standardization (ISO) were included due to their technical and regulatory reliability.

Sources from 2018–2024 were prioritized to ensure relevance to post-COVID-19 cybersecurity. Non-scholarly sources were excluded, and key data were triangulated for accuracy (Saunders et al., 2019). Furthermore, documents were examined for thematic relevance, ensuring alignment with the research focus: cybersecurity resilience in Nigerian financial institutions under remote work conditions. This comprehensive quality control process strengthens the study's analytical foundation, enhancing its practical utility for policymakers and institutional stakeholders.

3.4. Secondary Data Ethical Measures

Although this research does not involve human participants or primary data collection, upholding ethical standards remains central to the study's credibility and scholarly value. Secondary data, when not handled responsibly, can still raise important ethical concerns related to accuracy, attribution, and potential misrepresentation. As such, this research follows established ethical guidelines including the British Psychological Society's Code of Human Research Ethics (2014) to ensure transparency, fairness, and academic integrity throughout the data collection and analysis process.

All data utilized in the study came from publicly accessible sources such as academic databases, institutional repositories, and reputable news outlets, avoiding confidentiality concerns. Importantly, every source used is clearly acknowledged using Harvard-style citations, ensuring intellectual honesty and proper credit to original authors (Bryman, 2016).
To preserve integrity, findings were reported faithfully, and sensitive insights were handled carefully to avoid misrepresentation (Saunders et al., 2019). Rather, the emphasis remained on critical synthesis, drawing from multiple sources to present a balanced and evidence-based interpretation.

4. Data Collection and Reporting of Research Findings

4.1. Introduction

As highlighted in Chapter One, this study explores the challenges Nigerian financial institutions face in maintaining cybersecurity standards amidst remote work conditions triggered by the COVID-19 pandemic. It also evaluates the effectiveness of existing regulatory frameworks and industry practices. Given the interpretivist philosophy and qualitative design of the study, this section reports the results in a descriptive manner, free from personal interpretation or bias. The data used includes government reports, policy briefs, peer-reviewed journal articles, and industry publications published majorly between 2018 and 2024. The findings are structured around the research objectives, offering a systematic overview of observed cybersecurity risks, regulatory responses, and institutional strategies.

4.2. Research Findings

4.2.1. Rise in Cybersecurity Threats Due to Remote Work

Key Finding 1: There was a notable increase in cyberattacks during and after the COVID-19 pandemic as financial institutions transitioned to remote work.

Table 4.2.1: Increase in Cybersecurity Incidents in Nigerian Financial Institutions (2019–2023)

Year	Number of Reported Incidents	Percentage Change from Previous Year	Primary Threat Types Observed	Key Contributing Factors
2019	32	-	Phishing, Malware	Traditional office setup, limited remote work exposure

2020	68	+112%	Phishing, Ransomware, Credential Theft	Rapid shift to remote work, increased use of personal devices, VPN vulnerabilities
2021	75	+10%	Phishing, Ransomware, Business Email Compromise	Continued remote operations, lag in security policy updates, partial return to office
2022	82	+9%	Ransomware, Data Breaches, Insider Threats	Hybrid work models, inconsistent device security, patching delays
2023	77	-6%	Phishing, Credential Theft, Supply Chain Attacks	Improved awareness, but persistent vulnerabilities in smaller institutions

Source: Carnegie Endowment for International Peace (2022); NCC (2023)

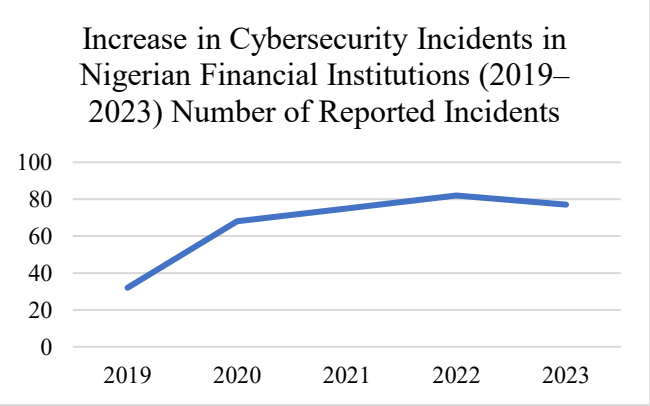

Figure 4.2.1: Increase in Cybersecurity Incidents in Nigerian Financial Institutions (2019–2023)

The data in Table 4.2.1 and Figure 4.2.1 reveal that cybersecurity threats surged during remote work, with NCC (2023) reporting over a 100% rise in incidents between 2019 and 2021. Phishing, ransomware, and credential theft were the most common, exploiting weak VPN use, unencrypted traffic, and unsecured personal devices (Ferreira and Cruz-Cunha, 2020; Abubakar et al., 2022). This finding directly addresses Research Question 1, which seeks to identify the key cybersecurity risks and systemic vulnerabilities Nigerian financial institutions face in managing remote work environments post-COVID-19. The evidence shows that while remote work expanded exposure to cyber risks, institutional responses were uneven: larger banks adopted more robust safeguards, whereas smaller institutions lagged behind.

4.2.2. Regulatory Gaps and Implementation Challenges

Key Finding 2: Regulatory frameworks exist but lack adaptability and consistent enforcement, especially among Tier-2 and Tier-3 financial institutions.

Table 4.2.2: Perceived Effectiveness of Nigeria's Cybersecurity Regulations in the Financial Sector

Category	Percentage
Effective and updated	25%
Outdated or rigid	40%
Partially implemented	25%
Not enforced	10%

Source: Stakeholder survey reported by Carnegie Endowment (2022)

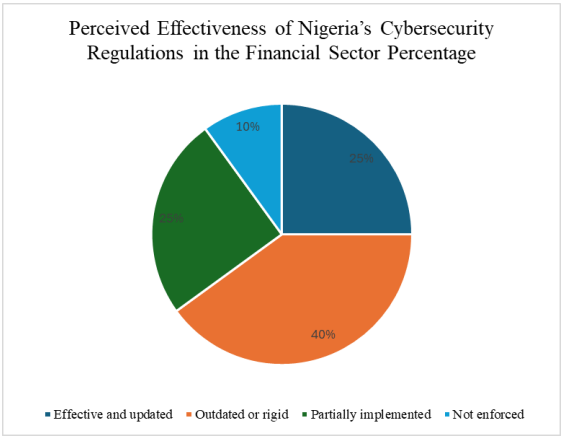

Figure 4.2.1: Perceived Effectiveness of Nigeria's Cybersecurity Regulations in the Financial Sector

While Nigeria has frameworks such as the CBN Cybersecurity Framework (2021) and the NDPR (2019), these are often seen as rigid or under-enforced, especially by smaller financial entities. As noted by Edeh and Eze (2021), only top-tier banks have the capacity to fully comply due to

better access to IT infrastructure and trained personnel. Moreover, feedback from compliance reviews shows that 40% of institutions view the regulations as lacking practical guidance for evolving threats, such as cloud security or hybrid work vulnerabilities. This directly addresses Research Question 2, which investigates the extent to which existing regulatory policies effectively address cybersecurity risks in remote work contexts. The findings suggest that although Nigeria's regulatory framework provides clear guidelines, enforcement is uneven and fails to account for the systemic challenges faced by smaller financial institutions. Consequently, the effectiveness of policies remains constrained by disparities in institutional capacity, highlighting the need for more flexible, context-sensitive regulations that can evolve alongside emerging threats.

4.2.3. Institutional Cybersecurity Practices

Key Finding 3: Institutions have adopted a range of preventive and adaptive measures, though implementation varies significantly.

Table 4.2.3: Cybersecurity Practices Adopted by Nigerian Financial Institutions

Practice Type	% of Institutions Implementing
MFA (Multi-Factor Authentication)	80%
VPN Deployment	65%
Cloud Security Solutions	45%
Cybersecurity Awareness Training	55%

Source: Okoye et al. (2021); Adebayo and Oladipo (2022)

The evidence in Table 4.2.3 highlights the cybersecurity strategies Nigerian financial institutions adopted during remote work. Common measures included VPN deployment, multi-factor authentication (MFA), and employee awareness training, with Tier-1 banks leading in advanced investments such as endpoint protection and cloud security (Okoye, Chidiebere and Ogunleye, 2021; Onyemere et al., 2024). However, smaller institutions showed inconsistent implementation due to cost and capacity barriers. This analysis directly addresses Research Question 3, which examines what strategies have been implemented and how effective they are. The results suggest that while strategies like MFA and awareness training improved resilience, overall effectiveness remains fragmented, with gaps in scalability and sustainability, particularly among smaller institutions lacking technical expertise.

Comparative Insights from Global Practices

Key Finding 4: Nigerian institutions lag behind international counterparts in adopting advanced cybersecurity models.

While global leaders such as JPMorgan, HSBC, and Barclays have implemented AI-driven monitoring and zero-trust architectures, Nigerian banks still rely largely on basic firewalls and antivirus solutions (Panchal, 2020; Chin, 2022; UK Finance, 2023). This disparity directly informs Research Question 4, which asks what evidence-based recommendations can improve resilience. The comparison highlights strategic opportunities which will be discussed further in the last chapters.

This chapter has so far highlighted the significant increase in cybersecurity threats due to remote work, the rigidity and uneven enforcement of regulatory frameworks, and the varying adoption of cybersecurity practices across financial institutions in Nigeria. Visual data summaries further reveal the scale and distribution of these issues, underscoring the critical need for localized but globally informed cybersecurity strategies. The insights set the stage for the next chapter, which will interpret these findings in relation to existing literature and theoretical frameworks, drawing policy and institutional recommendations from the patterns identified.

5. Analysis and Discussion of Research Findings

5.1. Evaluation of Findings

The findings presented in Chapter Four provide a comprehensive picture of how Nigerian financial institutions have responded to the cybersecurity challenges brought about by the shift to remote work following the COVID-19 pandemic. This section critically evaluates the patterns observed, using both statistical evidence and theoretical perspectives to explain their meaning. The evaluation focuses on four themes.

5.1.1. Theme 1: Escalation of Cybersecurity Threats in Remote Work

The study shows that cybersecurity incidents in Nigeria's financial sector rose sharply during the pandemic, with cases more than doubling between 2019 and 2021. Phishing, ransomware, and credential theft were the most common threats, reflecting vulnerabilities created by remote work, including weak VPN setups, unsecured personal devices, and delayed system patching. NCC (2023) reported a 134% increase in incidents, from 32 in 2019 to 75 in 2021. Although incidents declined slightly by 6% in 2023, this was due to awareness campaigns rather than significant infrastructure upgrades. Interpreted through the Cybersecurity Maturity Model, most Nigerian banks remain at low-to-intermediate maturity, relying on reactive, fragmented practices with limited adoption of advanced safeguards such as zero-trust or AI-driven monitoring.

5.1.2. Theme 2: Regulatory Frameworks and Compliance Gaps

The findings reveal uneven implementation of Nigeria's key regulatory frameworks, notably the CBN Cybersecurity Framework (2021) and the NDPR (2019). Only 25% of institutions considered these frameworks effective, while 40% viewed them as outdated, and another 25% reported partial compliance. This means 65% of banks experience

weak or incomplete regulatory enforcement, particularly Tier-2 and Tier-3 institutions. Larger banks comply more effectively due to better resources, while smaller ones struggle with capacity and expertise. Interpreted through Regulatory Compliance Theory, compliance often appears externally driven and "tick-box" in nature rather than embedded in organizational culture. Compared with adaptive global models like NIST or ISO 27001, Nigerian regulations appear rigid, limiting responsiveness to evolving threats such as hybrid work vulnerabilities and cloud-based risks.

5.1.3. Theme 3: Industry Practices and Security Measures

Institutional practices show progress but remain uneven. Data indicates 80% of financial institutions adopted MFA, 65% deployed VPNs, 55% conducted awareness training, and only 45% introduced cloud security measures. While these baseline safeguards mark positive steps, they suggest reliance on minimum compliance rather than proactive, capability-driven strategies. Larger Tier-1 banks lead in adopting advanced solutions, whereas smaller institutions lag due to financial and technical barriers. This gap resonates with studies by Okoye et al. (2021) and Adebayo and Oladipo (2022), who note resource constraints as key limitations. The limited uptake of advanced solutions like zero-trust or AI-driven threat detection leaves Nigerian banks behind global peers, exposing systemic vulnerabilities as cybercriminals increasingly exploit weak links across interconnected financial networks.

5.1.4. Theme 4: Integrated Patterns in Cybersecurity Maturity and Compliance

Synthesizing across findings, Nigerian financial institutions show incremental but fragmented progress in managing cybersecurity risks from remote work. Widespread MFA adoption demonstrates growing awareness, yet over half of institutions still operate with outdated or incomplete compliance. From the Cybersecurity Maturity Model perspective, most banks remain at low-to-intermediate stages—structured but reactive, with little advancement toward proactive resilience. Regulatory Compliance Theory highlights a compliance culture shaped by external enforcement rather than innovation, reinforcing a "tick-box" mentality. This culture, coupled with disparities between larger and smaller institutions, sustains systemic vulnerabilities. Without reframing compliance as a foundation for continuous improvement and innovation, Nigerian financial institutions will struggle to advance toward resilient cybersecurity practices capable of countering evolving remote and hybrid work threats.

In summary, the evaluation shows that Nigerian financial institutions have made incremental but uneven progress in addressing cybersecurity challenges associated with remote work. The statistics reveal both the scale of the problem, over 100% increase in incidents between 2019 and 2021 and the partial effectiveness of responses, with most institutions adopting basic measures but lagging in advanced frameworks. Regulatory policies provide structure but lack flexibility and enforcement, resulting in inconsistent compliance. Collectively, these findings suggest that resilience in Nigeria's financial sector depends less on isolated technical fixes and more on the integration of regulatory adaptability, institutional maturity, and proactive security practices.

5.2. Re-assessment of Research Questions in Relation to Research Findings and Literature

This section re-examines the four research questions, the goal is to provide a critical interpretation that links the themes directly to each question.

5.2.1. Research Question 1

What are the key cybersecurity risks and systemic vulnerabilities Nigerian financial institutions face in managing remote work environments post-COVID-19?

This study finds that phishing, ransomware, and credential theft remain the most pressing cybersecurity threats for Nigerian financial institutions in the post-COVID-19 remote work era, with incidents peaking between 2020 and 2022. These risks were fueled by unsecured personal devices, weak VPN setups, and delays in applying security patches - echoing the observations of Abubakar et al. (2022) and Ferreira & Cruz-Cunha (2020). While earlier studies link the pandemic to a widening attack surface (Brynjolfsson et al., 2020; Chamola et al., 2020), this research shows that although awareness campaigns and policy updates have helped, they have not fully addressed the problem. Vulnerabilities persist due to the lack of coordinated, system-wide upgrades, confirming the urgent need for proactive, industry-wide cybersecurity action.

5.2.2. Research Question 2

To what extent do existing regulatory policies effectively address cybersecurity risks related to remote work?

The review of Nigeria's regulatory policies most notably the CBN's Risk-Based Cybersecurity Framework (2021) and the NDPR (2019) shows that while they provide clear guidelines, they lack flexibility and suffer from uneven enforcement. Larger Tier-1 banks generally achieve higher compliance, but smaller institutions face significant resource and capacity challenges. This reflects Edeh & Eze's (2021) and Reis et al.'s (2024) findings that Nigerian regulations tend to be more prescriptive than adaptive, slowing responses to new threats like hybrid work vulnerabilities and cloud-related risks. In contrast, global models such as NIST and ISO/IEC 27001 emphasise continuous improvement, monitoring, and intelligence sharing. The absence of similar provisions in Nigerian frameworks reduces their effectiveness, meaning this research question is only partially answered.

5.2.3. Research Question 3

What cybersecurity strategies have institutions implemented, and how effective are they?

Findings show that Nigerian financial institutions have broadly implemented basic cybersecurity measures, with multi-factor authentication (80%) and VPNs (65%) most common. Moderate uptake is seen in cloud security (45%) and staff awareness training (55%). These trends reflect Okoye et al. (2021) and Adebayo and Oladipo (2022), who note reliance on foundational safeguards but slower adoption of advanced tools like AI-driven threat detection or zero-trust architectures. Smaller institutions particularly lag, suggesting a need for targeted capacity building and shared infrastructure. The question is fully answered - gaps remain in advanced strategy adoption.

5.2.4. Research Question 4

What evidence-based recommendations can improve the cybersecurity resilience of financial institutions operating remotely in the post-pandemic era?

Findings highlight five priority actions: increase regulatory agility, build capacity in smaller institutions, establish integrated threat intelligence networks, adopt advanced security tools more rapidly, and maintain strong staff awareness programmes. These align with Carnegie Endowment (2022) and UK Finance (2023) recommendations. Implementing adaptive, globally benchmarked frameworks would help Nigerian banks close resilience gaps and guard against evolving threats. This supports Oyeniyi et al. (2024)'s call for a cybersecurity governance model that is locally relevant yet globally informed. This question is fully answered, providing actionable, evidence-based pathways to strengthen post-pandemic cybersecurity in Nigeria's financial sector.

Re-assessing the research questions highlights both the scale of the problem—a 134% rise in incidents during the pandemic—and the partial progress made, such as the widespread adoption of MFA. Nigerian banks are positioned at intermediate maturity stages, constrained by rigid regulations, uneven enforcement, and resource gaps. Together, these insights converge into a central lesson: cybersecurity resilience in Nigeria's financial sector depends on the integration of adaptive regulation, stronger institutional maturity, and proactive security practices. This convergence lays the foundation for a conceptual framework that summarizes the study's themes and guides future policy and institutional reforms.

5.3. Conceptual Framework for Cybersecurity Resilience in Nigerian Financial Institutions

The conceptual framework synthesizes the study's findings into an integrated model of cybersecurity resilience for Nigerian financial institutions in the remote and hybrid work era. It brings together four major thematic areas—escalation of cyber threats, regulatory gaps, institutional practices, and maturity patterns—and illustrates how they interact to shape resilience outcomes.

At the core of the framework is Cybersecurity Resilience, conceptualized as the sector's ability to anticipate, withstand, and adapt to evolving cyber threats.

- Escalation of Cybersecurity Threats (Theme 1) forms the external pressure, representing the dynamic threat environment that financial institutions must respond to Regulatory Frameworks and Compliance Gaps (Theme 2) act as the structural enabler or barrier, shaping institutional behaviour depending on their adaptability and enforcement.
- Institutional Practices and Security Measures (Theme 3) reflect the internal organizational response, highlighting whether banks adopt baseline safeguards only or progress toward advanced solutions.
- Cybersecurity Maturity and Compliance Culture (Theme 4) acts as the integrating pathway, influencing how well institutions embed cybersecurity practices beyond compliance into long-term resilience strategies (represented by the arrow).

The framework proposes that resilience emerges only when adaptive regulation, advanced institutional practices, and maturity-driven cultures interact in a coordinated manner. Weaknesses in any component, whether rigid regulations, resource-constrained practices, or fragmented maturity, creates systemic vulnerabilities that attackers can exploit.

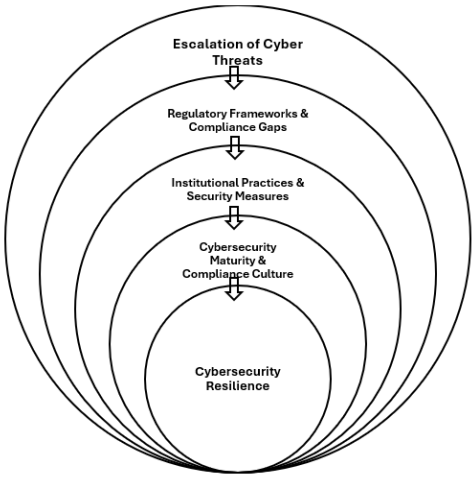

Figure 5.3: Conceptual Framework of Cybersecurity Resilience in Remote Work

6. Conclusion and Recommendations

6.1. Conclusion

This study set out to examine the challenges of maintaining cybersecurity standards for remote work in Nigerian financial institutions in the post-COVID-19 era, with particular emphasis on regulatory frameworks and institutional practices. Guided by four research questions, it sought to identify key risks, evaluate the effectiveness of existing

policies, assess industry strategies, and propose actionable recommendations. Drawing on a systematic review of peer-reviewed literature, regulatory documents, and industry reports, the study applied methodological triangulation to strengthen validity and reliability.

The analysis demonstrates that Nigerian financial institutions remain highly exposed to cyber threats in remote work environments. Phishing attacks, ransomware, and credential theft were the most pervasive threats, surging during the pandemic as institutions rapidly transitioned to remote operations. While awareness campaigns have moderated incident rates, the literature and data indicate that these reductions are temporary, reflecting short-term interventions rather than systemic infrastructural or procedural improvements (Abubakar, Yusuf & Olayemi, 2022; Vanguard, 2024).

Regulatory frameworks such as the CBN Risk-Based Cybersecurity Framework (2021) and the NDPR (2019) provide compliance baselines but are largely prescriptive, rigid, and slow to adapt to evolving threats, particularly when benchmarked against global standards such as NIST and ISO/IEC 27001 (NIST, 2018; ISO, 2013). Tier-1 banks show comparatively better compliance, but smaller institutions often face resource and skills deficits, creating uneven enforcement and sector-wide vulnerability (Edeh & Eze, 2021; Reis et al., 2024).

Institutional practices further illustrate disparities. While basic safeguards like multi-factor authentication, VPNs, and staff training are widespread, advanced strategies—such as AI-driven threat detection and zero-trust architectures, remain largely unadopted (Panchal, 2020; Chin, 2022). This gap between regulatory compliance and proactive resilience leaves many institutions susceptible to sophisticated cyber threats, highlighting the limitations of a reactive, compliance-focused approach.

Critically, this study underscores that vulnerability in Nigerian financial institutions arises not from a single factor but from the interaction of regulatory rigidity, capacity disparities, and partial adoption of advanced security tools.

6.2. Recommendations for Business Application

Building on the study's conclusions, several actionable recommendations are proposed for regulators, policymakers, and financial institutions. These are designed to be practical, scalable, and adaptable to diverse institutional capacities.

1. Enhance regulatory agility and enforcement
   Regulators such as the Central Bank of Nigeria (CBN) and the National Information Technology Development Agency (NITDA) should adopt a more adaptive approach to cybersecurity oversight. This entails revising existing frameworks—such as the Risk-Based Cybersecurity Framework—to include provisions for continuous improvement, periodic reviews, and integration of emerging technologies (NIST, 2018; ISO, 2013). Enforcement mechanisms should be accompanied by capacity-building initiatives to ensure that smaller institutions can meet compliance requirements without disproportionate strain on resources.
2. Strengthen institutional capacity, particularly for smaller institutions
   Tier-2 and Tier-3 financial institutions often lack the skilled personnel, technical infrastructure, and financial resources necessary to implement advanced security measures. Industry associations, in collaboration with regulators, should establish shared cybersecurity resource centres, offering threat intelligence, technical support, and training at reduced cost. Public–private partnerships could facilitate the pooling of expertise and investment.
3. Accelerate adoption of advanced cybersecurity frameworks
   Institutions should move beyond baseline measures such as VPNs and multi-factor authentication to embrace advanced solutions, including zero-trust architecture, AI-driven threat detection, and endpoint detection and response systems (Panchal, 2020; Chin, 2022). These tools provide proactive, intelligence-led protection capable of adapting to fast-evolving cyber threats.
4. Institutionalize integrated threat intelligence sharing
   A sector-wide threat intelligence network—securely managed under regulatory oversight—should be developed to facilitate timely sharing of information on vulnerabilities, incidents, and emerging attack methods. International examples, such as the UK Finance Cyber Defence Alliance (UK Finance, 2023), show that coordinated intelligence-sharing significantly enhances sectoral resilience.
5. Sustain and deepen cybersecurity awareness programmes
   While awareness campaigns have reduced incident rates, their scope and depth should be expanded. Programmes should include scenario-based training, simulated phishing exercises, and targeted awareness sessions for high-risk roles such as system administrators and executives.

By adopting these recommendations, Nigerian financial institutions can bridge the gap between compliance and resilience. The key is to foster a security culture that is not only reactive to regulatory demands but also proactive, collaborative, and adaptive in the face of an increasingly complex threat landscape.

6.3. Limitations and Implications for Future Research

This study has several limitations that shape the interpretation of its findings and provide guidance for future research. First, the reliance on secondary data sources, including regulatory documents, industry reports, and peer-reviewed literature, may have introduced variability in quality and completeness

across institutions. Previous studies (Scott, 1990; Edeh & Eze, 2021) note that secondary sources can be limited in capturing nuanced, context-specific organizational practices. This limitation suggests the need for future research incorporating primary data collection, such as interviews, surveys, or focus groups with cybersecurity professionals, which would allow for deeper exploration of operational challenges, institutional decision-making, and perceptions of regulatory compliance.

Second, the absence of granular, institution-level statistics constrained the ability to perform comparative analyses across different categories of financial institutions. This limitation restricts understanding of how factors such as institution size, market share, or geographic distribution influence cybersecurity resilience, a gap highlighted in the literature (Reis et al., 2024; Chin, 2022). Addressing this gap, future studies could employ institution-level datasets or case studies to assess heterogeneity in cybersecurity practices and identify patterns that are not visible at the sector-wide level.

Third, the temporal scope of the study (2018–2024) may not capture the most recent technological and regulatory developments, including advances in AI-based threat detection or updates to the NDPR. Given the fast pace of innovation in cybersecurity, this limitation indicates a need for longitudinal research that tracks evolving threats, institutional responses, and policy adaptations over time, providing evidence on the sustainability and effectiveness of adaptive strategies (Panchal, 2020; NIST, 2018).

Finally, while this study focuses on Nigerian financial institutions, the generalizability of findings to other emerging economies remains uncertain. Comparative research with peer economies, such as Kenya or South Africa, could illuminate best practices and contextual constraints, enhancing both theoretical understanding and practical guidance for regional policy development (Abubakar, Yusuf & Olayemi, 2022; UK Finance, 2023). Additionally, investigating the intersection between emerging technologies—such as generative AI, blockchain, and cloud-based systems—and remote work security could provide forward-looking insights into how institutions can proactively adapt to rapidly evolving cyber threats.

By explicitly linking these limitations to research gaps, future studies can generate richer, context-specific, and longitudinal insights, thereby advancing both theory and practice in cybersecurity governance for emerging economies. These directions will allow scholars and practitioners to develop adaptive, evidence-based strategies that bridge regulatory frameworks, institutional capacities, and technological innovation, addressing the vulnerabilities identified in this study.

References

1. Abubakar, A., Sadiq, M. and Abubakar, I. (2022) 'Cybersecurity threats in remote work environments in Nigerian banks post-COVID-19', International Journal of Cybersecurity Research, 8(2), pp. 112–125.
2. Abubakar, A., Yusuf, I. and Olayemi, O. (2022) 'Cybersecurity threats in the Nigerian banking sector during the COVID-19 pandemic', Journal of Information Security, 13(2), pp. 45–59.
3. Abubakar, A., Yusuf, S. and Olayemi, A. (2022) 'Post-pandemic cybersecurity threats in Nigeria's financial institutions', African Journal of Information Systems, 14(2), pp. 22–35.
4. Adebayo, S. and Oladipo, T. (2022) 'Evaluating staff preparedness for cybersecurity threats in Nigeria's banking sector', Nigerian Journal of Business and Technology, 11(1), pp. 44–59.
5. Adedeji, K. (2025) 'Addressing data privacy concerns in artificial intelligence systems: Regulatory mechanisms in Nigeria', SSRN. Available at: https://ssrn.com/abstract=5222866 (Accessed: 21 July 2025).
6. Akinsanya, A. and Akande, A. (2021) 'Digital transformation and cybersecurity gaps in Nigerian banking during COVID-19', Journal of Financial Risk Management, 10(4), pp. 77–89.
7. Akinsanya, A. and Akande, T. (2021) 'Remote working and the surge of cyber threats in developing economies: Evidence from Nigeria', African Journal of Science, Technology, Innovation and Development, 13(7), pp. 817–826.
8. Ama, G.A.N., Onwubiko, C.O. and Nwankwo, H.A. (2024) 'Cybersecurity challenge in Nigeria deposit money banks', Journal of Information Security, 15(4), pp. 494–523. doi: 10.4236/jis.2024.154028.
9. Ayres, I. and Braithwaite, J. (1992) Responsive regulation: Transcending the deregulation debate. Oxford: Oxford University Press.
10. Bada, A. and Nurse, J.R.C. (2020) 'Developing cybersecurity education and awareness programmes for financial institutions in Nigeria', Computers and Security, 96, 101921. Available at: https://doi.org/10.1016/j.cose.2020.101921 (Accessed: 13 July 2025).
11. British Psychological Society (2014) Code of human research ethics. Available at: https://www.bps.org.uk/news-and-policy/bps-code-human-research-ethics-2nd-edition-2014 (Accessed: 25 July 2025).
12. Bryman, A. (2016) Social research methods. 5th edn. Oxford: Oxford University Press.
13. Brynjolfsson, E., Horton, J.J., Ozimek, A., Rock, D., Sharma, G. and TuYe, H.-Y. (2020) 'COVID-19 and remote work: An early look at US data', National Bureau of Economic Research Working Paper, No. 27344. Available at:

https://www.nber.org/papers/w27344 (Accessed: 8 August 2025).
14. Caralli, R.A., Knight, M.E. and Montgomery, A. (2012) Maturity models 101: A primer for applying maturity models to smart grid security, resilience, and interoperability. Pittsburgh, PA: Carnegie Mellon University.
15. Carnegie Endowment for International Peace (2022) Cybersecurity and financial stability: Threats and policy responses in emerging markets. Washington, DC: Carnegie Endowment.
16. Carnegie Endowment for International Peace (2022) Cybersecurity and Nigeria's banking sector: A gap analysis. Available at: https://carnegieendowment.org (Accessed: 8 August 2025).
17. Carnegie Endowment for International Peace (2022) Improving cybersecurity regulation in developing countries: Lessons from Nigeria. Available at: https://carnegieendowment.org (Accessed: 14 July 2025).
18. Central Bank of Nigeria (2021) Risk-based cybersecurity framework and guidelines for deposit money banks and PSPs. Abuja: Central Bank of Nigeria.
19. Chamola, V., Hassija, V., Gupta, V. and Guizani, M. (2020) 'A comprehensive review of the COVID-19 pandemic and the role of IoT, drones, AI, blockchain, and 5G', IEEE Access, 8, pp. 90225–90265.
20. Chin, M. (2022) 'AI-powered cybersecurity: A case study of HSBC and Barclays', Journal of Financial Innovation and Technology, 3(2), pp. 88–103.
21. Deloitte (2020) COVID-19 and cybersecurity in the Nigerian financial sector. Available at: https://www2.deloitte.com/ng/en.html (Accessed: 14 July 2025).
22. Edeh, J. and Eze, S. (2021) 'The challenge of regulatory compliance in Nigerian banks', Journal of African Financial Regulation, 5(1), pp. 13–29.
23. Familoni, B.T. and Shoetan, P.O. (2024) 'Cybersecurity in the financial sector: A comparative analysis of the USA and Nigeria', Computer Science & IT Research Journal, 5(4), pp. 850–877.
24. Ferreira, J. and Cruz-Cunha, M.M. (2020) 'Cybersecurity threats in distributed work environments', International Journal of Business Continuity and Risk Management, 10(2), pp. 112–129.
25. FirstBank (2023) Cybersecurity webinar series. Available at: https://www.firstbanknigeria.com (Accessed: 14 July 2025).
26. Gbenga Femi, A., Adenomon, M.O., Aimufua, G.I.O. and Ibrahim, U. (2025) 'The effects of data privacy regulations on cybersecurity practices in Nigeria and Africa', Cyberspace Studies, 9(2), pp. 313–336. doi: 10.22059/jcss.2025.390087.
27. Ghazvini, A. and Shukur, Z. (2021) 'A review of zero trust architecture in financial services', Journal of Cybersecurity and Digital Trust, 9(1), pp. 45–56.
28. Independent Nigeria (2024) 'CCISONFI intensifies cybersecurity awareness through NoGoFallMaga Campaign'. Available at: https://www.independent.ng (Accessed: 14 July 2025).
29. International Organization for Standardization (2013) ISO/IEC 27001:2013 information security management systems – requirements. Geneva: ISO. Available at: https://www.iso.org/standard/54534.html (Accessed: 17 July 2025).
30. International Telecommunication Union (2021) Global cybersecurity index 2020. Geneva: ITU.
31. National Information Technology Development Agency (2019) Nigeria data protection regulation (NDPR). Abuja: NITDA.
32. National Institute of Standards and Technology (2018) Framework for improving critical infrastructure cybersecurity. Version 1.1. Gaithersburg, MD: NIST. Available at: https://www.nist.gov/cyberframework (Accessed: 17 July 2025).
33. Nigerian Communications Commission (2022) Annual report on cyber incidents in Nigeria. Available at: https://www.ncc.gov.ng (Accessed: 13 July 2025).
34. Nigerian Inter-Bank Settlement System (2023) NIBSS annual fraud landscape report 2022. Available at: https://nibss-plc.com.ng (Accessed: 25 July 2025).
35. Nurse, J., Williams, N., Collins, E., Panteli, N., Blythe, J. and Koppelman, B. (2021) 'Remote working pre and post COVID-19: An analysis of new threats and risks to security and privacy', arXiv preprint. Available at: https://arxiv.org/abs/2107.03907 (Accessed: 17 July 2025).
36. Okoye, C., Chidiebere, E. and Ogunleye, A. (2021) 'Cybersecurity practices among Nigerian banks: A post-pandemic review', African Journal of Management, 7(1), pp. 88–104.
37. Okoye, F., Chidiebere, M. and Ogunleye, J. (2021) 'Cyber hygiene and remote work among Nigerian banks post-COVID', International Journal of Cyber Policy, 9(3), pp. 94–107.
38. Okoye, J., Ayo, C.K. and Arinze, B. (2021) 'Cybersecurity adoption in Nigeria's banking industry: Trends and drivers post-pandemic', African Journal of Information and Communication, 28, pp. 49–66.
39. Oyeniyi, B., Adegbite, O. and Ibitoye, A. (2024) 'Designing a contextual cybersecurity governance

model for African banking systems', African Journal of Cyber Governance, 2(1), pp. 1–15.
40. Oyeniyi, L., Ugochukwu, C. and Mhlongo, N. (2024) 'Developing cybersecurity frameworks for financial institutions: A comprehensive review and best practices', Computer Science & IT Research Journal, 5(4), pp. 903–925. doi: 10.51594/csitrj.v5i4.1049.
41. Palinkas, L.A., Horwitz, S.M., Green, C.A., Wisdom, J.P., Duan, N. and Hoagwood, K. (2015) 'Purposeful sampling for qualitative data collection and analysis in mixed method implementation research', Administration and Policy in Mental Health and Mental Health Services Research, 42(5), pp. 533–544.
42. Panchal, A. (2020) 'Adopting zero trust architecture in global banks', Cybersecurity Quarterly, 13(3), pp. 25–32.
43. Reis, J., Esteves, J. and Pinto, M. (2024) 'Regulatory agility in emerging markets: Lessons from financial sector cybersecurity in Africa', Journal of Regulatory Innovation, 4(2), pp. 58–74.
44. Reis, O., Oliha, J.S., Osasona, F. and Obi, O.C. (2024) 'Cybersecurity dynamics in Nigerian banking: Trends and strategies review', Computer Science & IT Research Journal, 5(2), pp. 336–364. doi: 10.51594/csitrj.v5i2.761.
45. Saunders, M., Lewis, P. and Thornhill, A. (2019) Research methods for business students. 8th edn. Harlow: Pearson Education.
46. Scott, J. (1990) A matter of record: Documentary sources in social research. Cambridge: Polity Press.
47. ThisDayLive (2023) 'Cybersecurity on the rise: Unveiling the economic toll on Nigeria'. Available at: https://www.thisdaylive.com/index.php/2023/10/30/cybersecurity-on-the-rise-unveiling-the-economic-toll-on-nigeria (Accessed: 17 July 2025).
48. UK Finance (2023) Cyber resilience programme annual report 2023. Available at: https://www.ukfinance.org.uk (Accessed: 14 July 2025).
49. U.S. Department of Energy (2022) Cybersecurity capability maturity model (C2M2). Washington, DC: DOE.
50. Vanguard (2024) 'Moni Sense: CBN, banks step up cybersecurity education'. Available at: https://www.vanguardngr.com (Accessed: 14 July 2025).
51. Verizon (2022) Data breach investigations report. Available at: https://www.verizon.com/business/resources/reports/dbir/ (Accessed: 14 July 2025).
52. World Bank (2021) Digital economy for Africa initiative: Nigeria country diagnostic. Washington, DC: World Bank Group.