GENIUS MULTIDISCIPLINARY INTERNATIONAL JOURNAL
ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768555
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA
NASARAWA STATE UNIVERSITY KEFFI
GLOBAL PARTNER

EXAMINING THE REGULATORY FRAMEWORKS DRIVING CYBERSECURITY ADOPTION IN NIGERIAN FINANCIAL INSTITUTIONS

Aliyu Buba Dahiru[1] Mohammed Kabiru Halidu[2]

[1,2]Computer Engineering Department, Federal Polytechnic Mubi, Adamawa State, Nigeria

08036159158

Emails: 72moonali@gmail.com

Abstract

The rapid digitalization of financial services has transformed the operations of Nigerian financial institutions, improving efficiency and innovation while increasing exposure to cyber threats such as phishing, ransomware, data breaches, and financial fraud. To address these risks, Nigerian regulators have introduced legal and policy frameworks aimed at strengthening cybersecurity governance and encouraging the adoption of cybersecurity practices across the financial sector. This study examines the regulatory frameworks driving cybersecurity adoption in Nigerian financial institutions and assesses their role in enhancing cyber resilience and regulatory compliance. The study employs a qualitative doctrinal approach based on a review of relevant cybersecurity regulations, policy documents, academic literature, and industry reports published between 2020 and 2026. Key frameworks analyzed include the Cybercrimes (Prohibition, Prevention, etc.) Act, the Nigeria Data Protection Act 2023, the Central Bank of Nigeria's Risk-Based Cybersecurity Framework and Guidelines, and the National Cybersecurity Policy and Strategy. Institutional Theory provides the analytical lens for understanding how regulatory pressures influence organizational cybersecurity practices. The findings reveal that regulatory frameworks have significantly promoted cybersecurity adoption by strengthening governance structures, risk management processes, incident response capabilities, and data protection measures. However, challenges such as compliance costs, regulatory overlap, skills shortages, and evolving cyber threats continue to affect implementation. The study highlights the need for greater regulatory coordination and capacity building to sustain cybersecurity resilience in Nigeria's financial sector.

Keywords: Cybersecurity Adoption; Financial Institutions; Regulatory Frameworks; Cybersecurity Governance; Regulatory Compliance; Nigeria; Financial Sector Security

1. Introduction

The rapid advancement of digital technologies has transformed the global financial services industry, enabling financial institutions to deliver innovative products and

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768555
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

services through electronic platforms. In Nigeria, the adoption of digital banking, mobile financial services, fintech innovations, cloud computing, and electronic payment systems has significantly enhanced financial inclusion, operational efficiency, and customer experience. The increasing reliance on digital infrastructures has accelerated the growth of the Nigerian financial sector and strengthened its contribution to national economic development. However, the growing digitalization of financial services has also expanded the attack surface available to cybercriminals, exposing financial institutions to sophisticated cyber threats that threaten organizational assets, customer data, financial stability, and public trust (Bouveret, 2020; World Bank, 2022).

Cybersecurity has consequently emerged as a strategic priority for financial institutions worldwide. The financial sector remains one of the most targeted industries by cybercriminals due to the high value of financial assets, sensitive customer information, and interconnected digital systems that characterize modern banking operations. Recent years have witnessed an increase in cyberattacks involving ransomware, phishing, malware, insider threats, distributed denial-of-service attacks, and business email compromise schemes targeting financial institutions across both developed and developing economies (International Monetary Fund [IMF], 2024). These threats have become increasingly sophisticated, leveraging artificial intelligence, automation, and advanced social engineering techniques to exploit vulnerabilities in organizational systems and human behavior. The consequences of successful cyberattacks extend beyond direct financial losses to include reputational damage, regulatory penalties, operational disruptions, and erosion of consumer confidence.

Nigeria's financial sector has experienced significant growth in digital transformation, driven by increasing internet penetration, smartphone adoption, cashless policy initiatives, and the expansion of financial technology services. While these developments have created new opportunities for economic growth and financial inclusion, they have simultaneously heightened cybersecurity risks within the sector. Reports from industry stakeholders indicate that Nigerian financial institutions continue to face persistent cyber threats ranging from unauthorized access and identity theft to payment fraud and data breaches (Kshetri, 2021). As financial institutions increasingly depend on digital platforms to support critical operations, ensuring robust cybersecurity measures has become essential for maintaining operational resilience and protecting stakeholders from emerging cyber risks.

Recognizing the strategic importance of cybersecurity to national economic stability and financial system resilience, regulatory authorities in Nigeria have introduced a range of legal, policy, and institutional frameworks designed to strengthen cybersecurity governance and promote the adoption of cybersecurity practices among financial institutions. These frameworks establish mandatory requirements relating to information security governance, risk management, incident reporting, data protection, cyber resilience, and regulatory compliance. Notable regulatory instruments include the Cybercrimes (Prohibition, Prevention, etc.) Act, the Nigeria

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768555
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Data Protection Act 2023, the Central Bank of Nigeria's Risk-Based Cybersecurity Framework and Guidelines for Other Financial Institutions, and the National Cybersecurity Policy and Strategy. Collectively, these frameworks seek to enhance organizational preparedness against cyber threats while promoting accountability and responsible management of digital assets within the financial ecosystem.

The growing emphasis on cybersecurity regulation reflects a broader recognition that market-driven cybersecurity investments alone may be insufficient to address evolving cyber risks. Regulatory interventions serve as mechanisms through which governments and supervisory agencies encourage organizations to adopt minimum cybersecurity standards, strengthen governance structures, and implement appropriate controls to safeguard critical information assets. Institutional Theory suggests that organizations often respond to regulatory pressures by aligning their practices with established norms and compliance requirements, thereby improving organizational legitimacy and reducing exposure to legal and operational risks (Scott, 2022). Within the Nigerian financial sector, regulatory frameworks have increasingly become important drivers of cybersecurity adoption by influencing strategic decision-making, resource allocation, and organizational security culture.

Despite the existence of multiple cybersecurity regulations and guidelines, concerns remain regarding the effectiveness of implementation and compliance across the financial sector. Financial institutions continue to encounter challenges associated with regulatory complexity, overlapping compliance obligations, cybersecurity skills shortages, high implementation costs, and rapidly evolving threat landscapes. These challenges raise important questions regarding the extent to which existing regulatory frameworks effectively drive cybersecurity adoption and contribute to improved cyber resilience. Furthermore, the emergence of new technologies such as artificial intelligence, cloud computing, open banking, and digital currencies continues to introduce novel cybersecurity considerations that may require adaptive regulatory responses.

Against this backdrop, this study examines the regulatory frameworks driving cybersecurity adoption in Nigerian financial institutions. Specifically, the study explores the key regulatory instruments governing cybersecurity within the sector, analyzes their influence on organizational cybersecurity practices, and evaluates the challenges affecting their implementation and effectiveness. By providing a comprehensive assessment of the relationship between regulation and cybersecurity adoption, the study contributes to the growing body of knowledge on cybersecurity governance in emerging economies. The findings are expected to offer valuable insights for policymakers, regulators, cybersecurity professionals, and financial institutions seeking to strengthen cybersecurity resilience and promote sustainable digital transformation within Nigeria's financial sector.

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768555
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

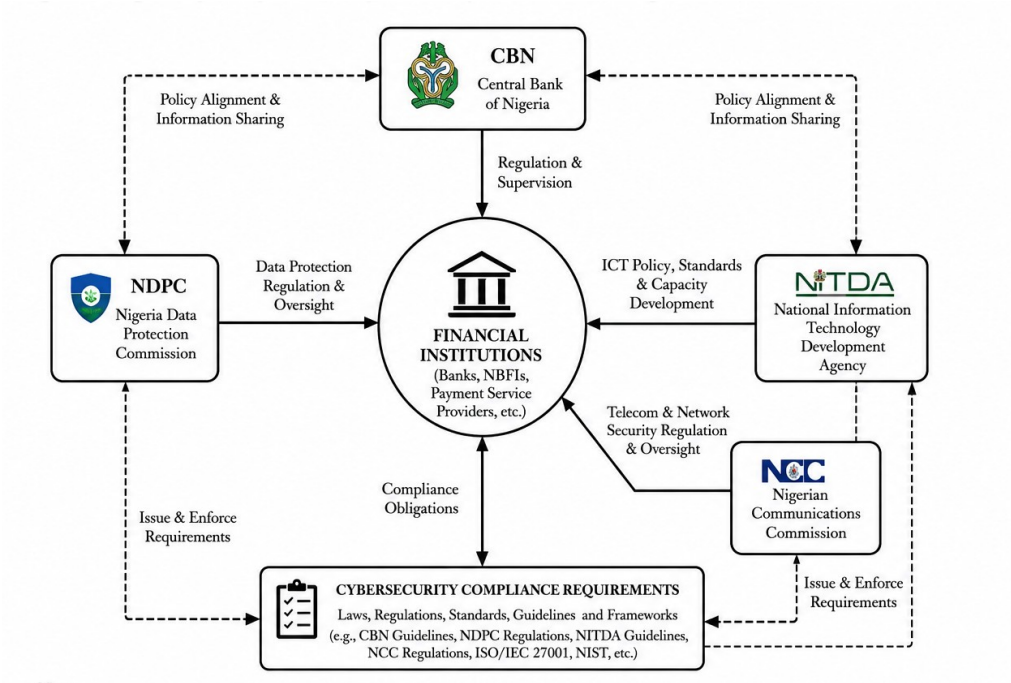

Figure 1. Regulatory Ecosystem for Cybersecurity Governance in Nigerian Financial Institutions

2. Literature Review

Cybersecurity has become a critical concern for organizations operating in increasingly digital environments, particularly within the financial services sector where the confidentiality, integrity, and availability of information assets are

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768555
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

fundamental to operational continuity and stakeholder trust. The concept of cybersecurity adoption refers to the extent to which organizations implement technological, organizational, and procedural measures designed to protect information systems, networks, and digital assets from cyber threats and vulnerabilities. Contemporary cybersecurity adoption extends beyond the deployment of security technologies to include governance structures, risk management frameworks, employee awareness programs, regulatory compliance mechanisms, and organizational cultures that support security-conscious behavior (Von Solms & Van Niekerk, 2021). As cyber threats continue to evolve in sophistication and frequency, organizations are increasingly recognizing cybersecurity as a strategic business imperative rather than merely a technical function.

The growing importance of cybersecurity adoption has been driven largely by the rapid digital transformation occurring across industries. Financial institutions have increasingly embraced digital technologies such as cloud computing, mobile banking, artificial intelligence, blockchain systems, and digital payment platforms to improve efficiency and customer service delivery. While these innovations have generated significant economic and operational benefits, they have simultaneously increased exposure to cyber risks. Researchers argue that digital transformation has expanded organizational attack surfaces, creating new vulnerabilities that cybercriminals can exploit through both technical and human-centered attack vectors (Bouveret, 2020). Consequently, organizations are investing more heavily in cybersecurity capabilities to safeguard critical assets and ensure operational resilience.

The financial services sector remains one of the most attractive targets for cybercriminals due to the concentration of valuable financial assets, sensitive customer information, and interconnected technological infrastructures. Recent studies indicate that cyberattacks against financial institutions have increased significantly in both frequency and complexity over the past decade (World Economic Forum, 2024). Common threats affecting financial institutions include phishing attacks, ransomware campaigns, malware infections, insider threats, credential theft, business email compromise, distributed denial-of-service attacks, and advanced persistent threats. These attacks can result in substantial financial losses, reputational damage, regulatory sanctions, service disruptions, and erosion of public confidence in financial systems.

Among the most prevalent threats facing financial institutions is phishing, which exploits human vulnerabilities through deceptive communications designed to obtain sensitive information such as passwords, account details, and authentication credentials. Phishing attacks have become increasingly sophisticated with the use of artificial intelligence and social engineering techniques that make fraudulent communications more convincing and difficult to detect (Verizon, 2024). Similarly, ransomware attacks have emerged as a major cybersecurity challenge for financial institutions globally. These attacks involve the encryption of organizational data or systems, followed by demands for financial payment in exchange for restoration of access. The increasing sophistication of ransomware groups and the emergence of ransomware-as-a-service business models have significantly elevated the threat landscape for financial institutions (ENISA, 2023).

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768555
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Insider threats represent another significant cybersecurity concern within the financial sector. Unlike external attackers, insider threats originate from employees, contractors, or authorized individuals who intentionally or unintentionally compromise organizational security. Studies have shown that insider threats can be particularly difficult to detect because perpetrators often possess legitimate access to organizational systems and information resources (Greitzer & Frincke, 2021). Additionally, the growing adoption of third-party service providers and cloud-based infrastructures has introduced new supply-chain vulnerabilities that may expose financial institutions to indirect cybersecurity risks. Consequently, cybersecurity strategies increasingly emphasize comprehensive risk management approaches that address both internal and external threat vectors.

The relationship between cybersecurity adoption and regulatory compliance has attracted considerable attention within contemporary cybersecurity literature. Regulatory compliance refers to the process through which organizations adhere to laws, regulations, standards, and guidelines established by governmental authorities and industry regulators. Within the cybersecurity domain, regulations serve as instruments for promoting minimum security standards, enhancing organizational accountability, and reducing systemic cyber risks across critical sectors. Scholars have argued that regulatory requirements often function as catalysts for cybersecurity investments by compelling organizations to implement security controls that they might otherwise underinvest in due to cost considerations or competing strategic priorities (Kshetri, 2021).

Governance, Risk, and Compliance (GRC) frameworks have emerged as important mechanisms through which organizations align cybersecurity objectives with regulatory requirements and business goals. Effective cybersecurity governance involves the establishment of leadership structures, policies, and oversight mechanisms that support informed decision-making regarding cybersecurity risks. Risk management processes enable organizations to identify, assess, and mitigate threats that could adversely affect operations, while compliance functions ensure adherence to applicable legal and regulatory obligations (ISACA, 2023). Within financial institutions, these components collectively contribute to organizational cybersecurity maturity by fostering a proactive and systematic approach to cyber risk management.

Theoretical perspectives provide valuable insights into understanding the factors that drive cybersecurity adoption within regulated environments. Institutional Theory has emerged as one of the most widely applied frameworks for explaining organizational responses to regulatory pressures. According to Institutional Theory, organizations operate within broader institutional environments that shape behavior through formal rules, social expectations, and normative standards (Scott, 2022). The theory identifies three principal mechanisms through which institutional pressures influence organizational actions: coercive, normative, and mimetic pressures. Coercive pressures arise from legal and regulatory requirements imposed by governments and regulatory agencies. Normative pressures originate from professional standards, industry expectations, and best practices, while mimetic pressures occur when organizations imitate successful practices adopted by peers in response to uncertainty.

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768555
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

The application of Institutional Theory to cybersecurity governance suggests that organizations adopt cybersecurity measures not solely because of technical necessity but also due to external pressures that encourage conformity to accepted standards and regulatory expectations. In highly regulated sectors such as financial services, coercive pressures often play a particularly significant role in shaping cybersecurity practices. Regulatory agencies establish requirements relating to information security governance, incident reporting, risk management, and data protection, thereby compelling organizations to adopt cybersecurity controls necessary for compliance. At the same time, financial institutions may emulate cybersecurity practices implemented by leading organizations within the sector to maintain competitiveness and legitimacy. Institutional Theory therefore provides a useful framework for examining how regulatory frameworks influence cybersecurity adoption within Nigerian financial institutions.

Empirical studies conducted in recent years have increasingly examined the effectiveness of cybersecurity regulations in promoting organizational security practices. Research by Kshetri (2021) found that regulatory interventions play a significant role in encouraging cybersecurity investments and strengthening organizational resilience, particularly in developing economies where cybersecurity capabilities may be less mature. Similarly, World Bank (2022) studies on digital development highlighted the importance of regulatory frameworks in establishing trust within digital financial ecosystems and supporting sustainable technological innovation. These findings suggest that effective cybersecurity regulations can create incentives for organizations to prioritize cybersecurity investments while enhancing overall sectoral resilience.

Studies focusing specifically on the financial sector indicate that cybersecurity regulations contribute to improved governance structures, enhanced risk management practices, and stronger incident response capabilities. Bouveret (2020) observed that regulatory requirements have become increasingly important in reducing systemic cyber risks within financial systems by promoting standardized approaches to cybersecurity management. Furthermore, research conducted by the International Monetary Fund (2024) emphasizes that cyber resilience within financial institutions depends significantly on the effectiveness of regulatory oversight and the capacity of institutions to implement mandated security controls. These findings underscore the growing recognition of cybersecurity regulation as an essential component of financial sector stability.

Within the Nigerian context, emerging literature has examined the evolving cybersecurity landscape and the role of regulatory institutions in addressing cyber risks. Scholars have noted that the expansion of digital banking services, fintech innovations, and electronic payment systems has increased the importance of cybersecurity governance within the country's financial sector (Awoleye et al., 2023). Recent studies suggest that regulatory frameworks introduced by the Central Bank of Nigeria and other relevant authorities have contributed to increased awareness of cybersecurity risks and encouraged financial institutions to strengthen cybersecurity governance practices. However, researchers also identify persistent challenges including limited cybersecurity expertise, compliance costs, technological constraints,

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768555
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

and fragmented regulatory oversight that may hinder effective implementation of cybersecurity requirements.

Although existing literature demonstrates the importance of regulatory frameworks in promoting cybersecurity adoption, significant gaps remain regarding the specific mechanisms through which regulations influence cybersecurity practices within Nigerian financial institutions. Much of the available research focuses either on general cybersecurity challenges or broader regulatory developments without providing comprehensive analysis of how multiple regulatory frameworks collectively shape organizational cybersecurity behavior. Furthermore, the introduction of new regulatory instruments, including the Nigeria Data Protection Act 2023 and updated cybersecurity guidelines, has created a need for contemporary assessments of regulatory effectiveness. Addressing these gaps is important for understanding the extent to which regulatory frameworks contribute to cybersecurity adoption and cyber resilience within Nigeria's rapidly evolving financial ecosystem.

3. Regulatory Frameworks Governing Cybersecurity in Nigerian Financial Institutions

The increasing digitization of financial services in Nigeria has necessitated the development of regulatory frameworks aimed at strengthening cybersecurity governance and protecting critical financial infrastructures from cyber threats. As financial institutions continue to expand their reliance on digital technologies, regulators have recognized the need to establish legal, policy, and operational mechanisms that promote cybersecurity adoption, enhance cyber resilience, and mitigate systemic risks. Consequently, Nigeria has developed a multi-layered cybersecurity regulatory environment comprising legislation, sector-specific guidelines, national policies, and institutional oversight mechanisms. These frameworks collectively influence how financial institutions design, implement, and maintain cybersecurity programs while ensuring compliance with national and international security standards.

One of the most significant legal instruments governing cybersecurity in Nigeria is the Cybercrimes (Prohibition, Prevention, etc.) Act. Originally enacted to combat cybercrime and strengthen national cybersecurity capabilities, the Act provides a legal foundation for addressing cyber-related offenses, protecting critical national information infrastructure, and promoting cybersecurity accountability across organizations. The legislation imposes obligations on organizations to implement security measures capable of protecting information systems and supporting cybercrime investigations. For financial institutions, the Act establishes expectations relating to cyber incident reporting, digital evidence preservation, and cooperation with law enforcement agencies during cybersecurity investigations. By creating legal consequences for cybercrime activities and encouraging preventive security measures, the Act serves as an important regulatory driver of cybersecurity adoption within the financial sector.

Another significant development in Nigeria’s cybersecurity regulatory landscape is the enactment of the Nigeria Data Protection Act 2023. The Act represents a major advancement in data governance by establishing comprehensive legal requirements

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768555
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

for the processing, storage, protection, and transfer of personal data. Financial institutions routinely collect and process large volumes of customer information, making data protection a critical component of cybersecurity governance. The Act requires organizations to implement appropriate technical and organizational measures to protect personal data against unauthorized access, disclosure, alteration, or destruction. It also introduces obligations relating to breach notification, accountability, privacy governance, and risk assessment. These requirements have encouraged financial institutions to strengthen cybersecurity controls, improve data management practices, and integrate privacy considerations into broader cybersecurity strategies. As a result, the Act functions not only as a data protection framework but also as a catalyst for cybersecurity investment and organizational security maturity.

Within the financial sector specifically, the Central Bank of Nigeria (CBN) plays a pivotal role in promoting cybersecurity adoption through sector-specific regulations and supervisory mechanisms. The CBN's Risk-Based Cybersecurity Framework and Guidelines for Other Financial Institutions establish comprehensive cybersecurity requirements designed to enhance cyber resilience across regulated entities. The framework emphasizes the importance of cybersecurity governance, risk management, security monitoring, incident response, business continuity planning, and third-party risk management. It requires financial institutions to develop cybersecurity strategies aligned with organizational objectives, establish board-level oversight of cybersecurity risks, and implement continuous monitoring mechanisms capable of identifying and responding to emerging threats.

The risk-based approach adopted by the CBN recognizes that cybersecurity threats vary across institutions depending on organizational size, complexity, and technological exposure. Consequently, financial institutions are expected to assess cybersecurity risks continuously and implement controls proportionate to their risk profiles. This approach encourages organizations to move beyond compliance-oriented security practices toward more proactive and adaptive cybersecurity management. Furthermore, the framework promotes regular security assessments, penetration testing, vulnerability management, and incident reporting, thereby enhancing organizational preparedness against cyber threats. Through these requirements, the CBN has significantly influenced cybersecurity adoption by embedding cybersecurity considerations within broader risk management and corporate governance structures.

At the national level, the National Cybersecurity Policy and Strategy provides strategic direction for cybersecurity development and cyber resilience across critical sectors, including finance. The policy recognizes cybersecurity as a national security and economic development priority and outlines objectives for strengthening cyber defense capabilities, improving public-private collaboration, promoting cybersecurity awareness, and enhancing critical infrastructure protection. For financial institutions, the policy reinforces the importance of adopting internationally recognized cybersecurity standards and participating in coordinated efforts to address emerging cyber threats. It also supports information sharing and collaboration among government agencies, regulators, and private sector organizations, thereby contributing to a more resilient cybersecurity ecosystem.

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768555
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

The Nigerian cybersecurity regulatory environment is further strengthened through the activities of multiple regulatory and supervisory institutions. The Nigeria Data Protection Commission oversees compliance with data protection requirements and promotes responsible data governance practices. The National Information Technology Development Agency contributes to cybersecurity governance through the development of information security standards and digital economy initiatives. The Nigerian Communications Commission supports cybersecurity efforts by regulating telecommunications infrastructure and promoting secure digital communications, while the Securities and Exchange Commission increasingly emphasizes cybersecurity governance among capital market participants. Together, these institutions contribute to a comprehensive regulatory ecosystem that shapes cybersecurity expectations across the financial sector.

Despite the significant progress achieved through these frameworks, the multiplicity of regulatory actors can create compliance challenges for financial institutions. Organizations may be required to satisfy overlapping obligations relating to cybersecurity governance, risk management, incident reporting, and data protection. While these overlapping requirements often reinforce cybersecurity objectives, they may also increase compliance complexity and operational costs. Nevertheless, the collective influence of these frameworks has contributed to greater cybersecurity awareness, improved governance practices, and increased investment in cybersecurity capabilities across Nigerian financial institutions.

Table 3: Comparison of Major Cybersecurity Regulations Affecting Financial Institutions in Nigeria

Regulation/Framework	Regulatory Authority	Key Cybersecurity Requirements	Influence on Cybersecurity Adoption
Cybercrimes (Prohibition, Prevention, etc.) Act	Federal Government of Nigeria	Cybercrime prevention, incident reporting, infrastructure protection	Strengthens legal accountability and security compliance
Nigeria Data Protection Act 2023	Nigeria Data Protection Commission	Data protection, breach notification, privacy governance	Enhances security controls and data governance
Risk-Based Cybersecurity Framework and Guidelines	Central Bank of Nigeria	Risk management, governance, monitoring, incident response	Promotes institutional cyber resilience and maturity
National Cybersecurity Policy and Strategy	Federal Government of Nigeria	National cyber resilience, collaboration, capacity building	Encourages strategic cybersecurity adoption
Information Security and Digital Governance Initiatives	NITDA, NCC, SEC	Security standards, digital infrastructure protection	Supports sector-wide cybersecurity implementation

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768555
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

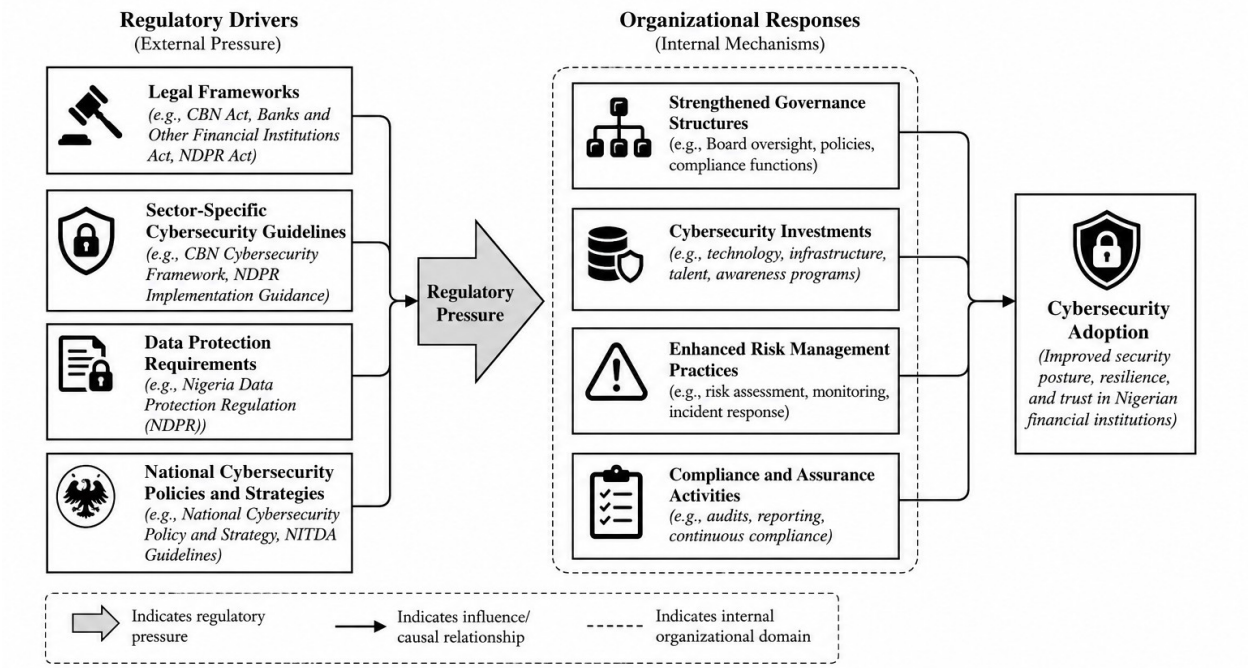

Figure 2: Regulatory Drivers of Cybersecurity Adoption in Nigerian Financial Institutions

The cumulative effect of these regulatory frameworks demonstrates that cybersecurity adoption within Nigerian financial institutions is increasingly driven by a combination of legal obligations, supervisory expectations, and strategic national priorities. Rather than functioning as isolated instruments, these frameworks collectively establish a governance environment that encourages organizations to strengthen cybersecurity capabilities, improve risk management practices, and enhance resilience against evolving cyber threats. Their continued effectiveness, however, depends on regulatory coordination, institutional capacity, and the ability of financial institutions to adapt to an increasingly dynamic cybersecurity landscape.

4. Methodology

This study adopts a qualitative research approach to examine the regulatory frameworks driving cybersecurity adoption in Nigerian financial institutions. The choice of a qualitative methodology is informed by the exploratory and analytical nature of the research, which seeks to understand how legal, regulatory, and policy instruments influence cybersecurity governance and organizational security practices within the financial sector. Qualitative research is particularly appropriate for studies that aim to analyze complex institutional, regulatory, and governance issues where contextual understanding is essential. Rather than relying on numerical measurements, the study focuses on the interpretation of regulatory documents, policy frameworks, academic literature, and institutional reports to generate comprehensive insights into the relationship between regulation and cybersecurity adoption.

The study employs a doctrinal research design complemented by a systematic review of relevant literature. Doctrinal research is widely used in legal and policy studies to

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768555
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

examine existing laws, regulations, policies, and institutional frameworks governing a particular subject area. In the context of cybersecurity governance, this approach enables a detailed examination of the legal and regulatory instruments that shape cybersecurity practices within Nigerian financial institutions. The design is particularly suitable because the study seeks to evaluate the content, objectives, implementation mechanisms, and cybersecurity implications of regulatory frameworks rather than measure organizational behavior through surveys or experiments. By integrating doctrinal analysis with contemporary scholarly literature, the study provides both regulatory and theoretical perspectives on cybersecurity adoption.

Data for the study were obtained from secondary sources. The primary sources consisted of relevant cybersecurity laws, regulations, policy documents, and regulatory guidelines applicable to Nigerian financial institutions. These included the Cybercrimes (Prohibition, Prevention, etc.) Act, the Nigeria Data Protection Act 2023, the Central Bank of Nigeria's Risk-Based Cybersecurity Framework and Guidelines for Other Financial Institutions, and the National Cybersecurity Policy and Strategy. Additional regulatory materials published by agencies such as the Nigeria Data Protection Commission, the National Information Technology Development Agency, the Nigerian Communications Commission, and the Securities and Exchange Commission were also reviewed. These documents provided authoritative information regarding regulatory requirements, compliance obligations, cybersecurity governance expectations, and institutional responsibilities.

To complement the regulatory review, the study examined peer-reviewed journal articles, conference proceedings, industry reports, policy analyses, and publications from international organizations published between 2020 and 2026. Particular attention was given to studies focusing on cybersecurity governance, regulatory compliance, cyber resilience, financial sector cybersecurity, and digital transformation. The inclusion of recent literature ensured that the analysis reflected contemporary developments in cybersecurity regulation and emerging challenges affecting financial institutions. Sources were selected based on relevance, credibility, and contribution to understanding the relationship between cybersecurity regulation and organizational adoption practices.

Data collection was conducted through a structured document review process. Relevant documents were identified through academic databases, institutional repositories, regulatory websites, government publications, and reports from international organizations. The selection process prioritized documents that directly addressed cybersecurity governance, financial sector regulation, cyber risk management, data protection, and regulatory compliance. Following identification, the documents were reviewed systematically to extract information relating to regulatory objectives, cybersecurity requirements, implementation mechanisms, compliance obligations, and reported outcomes. This approach facilitated the organization of data into themes that supported the objectives of the study.

The collected data were analyzed using thematic analysis. Thematic analysis is a qualitative analytical technique that involves identifying, organizing, and interpreting recurring patterns within textual data. In this study, the analysis focused on identifying major themes relating to regulatory influence on cybersecurity adoption, governance

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768555
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

requirements, compliance mechanisms, cyber resilience, implementation challenges, and emerging regulatory trends. The identified themes were subsequently examined through the lens of Institutional Theory to explain how regulatory pressures shape organizational cybersecurity behavior. The use of Institutional Theory provided a conceptual framework for understanding the influence of coercive, normative, and mimetic pressures on cybersecurity adoption within financial institutions.

To enhance the credibility and reliability of the findings, the study relied on authoritative and verifiable sources, including official regulatory documents, government publications, and peer-reviewed academic literature. The use of multiple data sources facilitated triangulation, thereby reducing the risk of bias associated with reliance on a single source of information. Furthermore, the study adhered to accepted principles of academic integrity through proper attribution of sources and objective interpretation of findings. Since the research was based exclusively on publicly available documents and secondary data, no human participants were involved, and no ethical risks requiring formal ethical approval were identified. This methodological approach provides a robust foundation for examining the regulatory frameworks driving cybersecurity adoption in Nigerian financial institutions and for evaluating their effectiveness in promoting cyber resilience and regulatory compliance.

5. Findings and Discussion

The findings of this study reveal that cybersecurity adoption within Nigerian financial institutions is increasingly influenced by a combination of legal obligations, regulatory expectations, and institutional pressures. The analysis of relevant regulatory frameworks demonstrates that cybersecurity has evolved from a predominantly technical concern into a strategic governance issue requiring active involvement from senior management, boards of directors, regulators, and external stakeholders. The reviewed regulations collectively establish minimum cybersecurity requirements while encouraging organizations to adopt proactive measures for identifying, managing, and mitigating cyber risks. The findings further indicate that regulatory frameworks have become significant mechanisms through which cybersecurity awareness, investment, and organizational accountability are promoted across the Nigerian financial sector.

A major finding of the study is that regulatory compliance has emerged as one of the most important drivers of cybersecurity adoption among financial institutions. The regulatory environment created by cybersecurity legislation, data protection requirements, and sector-specific guidelines compels institutions to establish cybersecurity programs capable of meeting mandatory compliance obligations. This finding supports the assumptions of Institutional Theory, particularly the concept of coercive pressure, which suggests that organizations adopt specific practices in response to formal rules and regulatory expectations. Financial institutions are increasingly required to implement cybersecurity policies, conduct risk assessments, establish incident response procedures, and maintain adequate security controls to satisfy regulatory requirements. Consequently, cybersecurity adoption is no longer driven solely by organizational discretion but has become an essential component of regulatory compliance and corporate governance.

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768555
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

The findings indicate that compliance requirements have encouraged greater investment in cybersecurity technologies and governance structures. Many financial institutions have strengthened security monitoring capabilities, implemented advanced authentication mechanisms, expanded vulnerability management programs, and improved cybersecurity training initiatives. Regulatory requirements relating to cybersecurity governance have also elevated the role of boards and senior executives in cybersecurity decision-making. This development reflects a broader shift toward recognizing cybersecurity as an enterprise-wide risk management issue rather than a responsibility confined to information technology departments. As organizations strive to avoid regulatory sanctions, reputational damage, and operational disruptions, compliance obligations increasingly serve as incentives for sustained cybersecurity investments.

Another important finding relates to the influence of the Central Bank of Nigeria's cybersecurity regulations on organizational cybersecurity maturity. The analysis suggests that the CBN's Risk-Based Cybersecurity Framework and Guidelines have significantly contributed to the institutionalization of cybersecurity governance within financial institutions. By requiring organizations to establish formal cybersecurity governance structures, conduct risk-based assessments, and implement continuous monitoring mechanisms, the framework has encouraged a more structured and strategic approach to cybersecurity management. Financial institutions are increasingly integrating cybersecurity considerations into broader enterprise risk management processes, thereby improving organizational preparedness against cyber threats.

The adoption of risk-based cybersecurity practices has enhanced the ability of institutions to identify vulnerabilities, prioritize security investments, and allocate resources according to risk exposure. This finding aligns with contemporary cybersecurity governance literature, which emphasizes the importance of risk-based approaches in improving organizational cyber resilience. Rather than applying uniform security controls across all systems, financial institutions are increasingly tailoring cybersecurity measures to address specific threats, business processes, and operational environments. Such practices contribute to greater efficiency in cybersecurity resource allocation while improving overall security effectiveness. Furthermore, mandatory incident reporting requirements have strengthened communication between financial institutions and regulatory authorities, enabling more coordinated responses to emerging cyber threats.

The study also reveals that data protection regulations have become significant contributors to cybersecurity adoption within Nigerian financial institutions. The implementation of the Nigeria Data Protection Act 2023 has expanded organizational responsibilities relating to personal data protection, privacy governance, and breach management. Financial institutions process substantial volumes of sensitive customer information, making compliance with data protection requirements both a legal obligation and a business necessity. The findings indicate that organizations have increasingly adopted technical and organizational safeguards to ensure compliance with data protection requirements, including enhanced access controls, encryption technologies, data classification procedures, and security awareness programs.

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768555
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Beyond regulatory compliance, data protection obligations have encouraged organizations to develop stronger information governance frameworks and accountability mechanisms. The requirement to report data breaches and demonstrate compliance with privacy principles has increased organizational attention to cybersecurity risks associated with data handling and storage. This finding supports existing literature suggesting that privacy regulations often generate positive cybersecurity outcomes by encouraging organizations to strengthen information security practices. In the Nigerian financial sector, the integration of privacy and cybersecurity objectives appears to be contributing to more comprehensive approaches to digital risk management.

Despite these positive developments, the findings identify several challenges affecting the effectiveness of cybersecurity regulations and their influence on cybersecurity adoption. One of the most frequently observed challenges is the high cost associated with regulatory compliance. Implementing cybersecurity technologies, conducting security assessments, maintaining monitoring systems, and employing qualified cybersecurity professionals require substantial financial investments. While larger financial institutions may possess the resources necessary to satisfy regulatory requirements, smaller institutions may face greater difficulties in achieving and maintaining compliance. This disparity has the potential to create uneven levels of cybersecurity maturity across the financial sector.

Another significant challenge concerns the shortage of skilled cybersecurity professionals. Effective implementation of cybersecurity frameworks requires specialized expertise in areas such as threat intelligence, incident response, vulnerability management, digital forensics, and security governance. However, many organizations continue to experience difficulties attracting and retaining qualified cybersecurity personnel. The global shortage of cybersecurity professionals further exacerbates this challenge, limiting the capacity of institutions to implement advanced security controls and respond effectively to evolving threats. Consequently, regulatory requirements alone may be insufficient to achieve desired cybersecurity outcomes without parallel investments in workforce development and capacity building.

The findings also indicate that overlapping regulatory responsibilities among different agencies may create compliance complexities for financial institutions. Multiple regulators oversee various aspects of cybersecurity, data protection, digital governance, telecommunications security, and financial sector supervision. Although these regulatory efforts are generally complementary, institutions may encounter challenges in interpreting and satisfying multiple compliance requirements simultaneously. Regulatory fragmentation can increase administrative burdens and create uncertainty regarding implementation priorities. This finding suggests that greater regulatory coordination and harmonization may enhance compliance efficiency while reducing duplication of effort.

Additionally, the rapidly evolving nature of cyber threats continues to challenge the effectiveness of existing regulatory frameworks. Cybercriminals increasingly employ sophisticated techniques involving artificial intelligence, automation, and advanced social engineering tactics. As technological innovation accelerates, regulatory frameworks must continuously adapt to address emerging risks associated with cloud

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768555
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

computing, open banking, digital currencies, artificial intelligence applications, and interconnected financial technologies. Static regulatory approaches may struggle to keep pace with these developments, highlighting the importance of flexible and adaptive cybersecurity governance models.

The findings further suggest that regulatory frameworks contribute to cybersecurity adoption not only through enforcement mechanisms but also through normative and mimetic institutional pressures. Financial institutions increasingly recognize cybersecurity as a critical component of organizational legitimacy and stakeholder confidence. Compliance with recognized cybersecurity standards signals commitment to security, risk management, and responsible governance. Organizations often benchmark their cybersecurity practices against industry peers and leading institutions, thereby facilitating the diffusion of cybersecurity best practices across the sector. These dynamics reinforce the broader institutional environment supporting cybersecurity adoption and organizational resilience.

Table 4: **Key Findings and Policy Implications**

Key Finding	Regulatory Implication	Organizational Impact
Regulatory compliance drives cybersecurity adoption	Continued enforcement and oversight are necessary	Increased cybersecurity investment and governance maturity
CBN cybersecurity guidelines strengthen cyber resilience	Sector-specific regulation remains critical	Improved risk management and incident response capabilities
Data protection requirements enhance security controls	Privacy and cybersecurity regulations should remain integrated	Stronger data governance and customer trust
Skills shortages affect implementation effectiveness	Capacity-building initiatives are required	Improved cybersecurity workforce readiness
Regulatory overlap creates compliance complexity	Greater coordination among regulators is needed	Reduced compliance burden and enhanced efficiency
Emerging technologies introduce new cyber risks	Adaptive and future-oriented regulations are necessary	Enhanced resilience against evolving threats

The findings demonstrate that regulatory frameworks have become fundamental drivers of cybersecurity adoption in Nigerian financial institutions. Through legal mandates, supervisory requirements, and institutional pressures, these frameworks have encouraged organizations to strengthen governance structures, improve cybersecurity capabilities, and enhance cyber resilience. However, the effectiveness of these frameworks depends not only on regulatory enforcement but also on the availability of organizational resources, cybersecurity expertise, and coordinated regulatory approaches capable of responding to an increasingly dynamic threat environment. The findings therefore suggest that sustained cybersecurity resilience within the Nigerian financial sector will require continuous collaboration among regulators, financial institutions, policymakers, and cybersecurity professionals.

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768555
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

6. Conclusion

This study examined the role of regulatory frameworks in driving cybersecurity adoption within Nigerian financial institutions and their influence on cybersecurity governance, risk management, and organizational resilience. The findings indicate that key regulatory instruments, including the Cybercrimes Act, the Nigeria Data Protection Act 2023, the Central Bank of Nigeria's Risk-Based Cybersecurity Framework, and the National Cybersecurity Policy and Strategy, have significantly strengthened cybersecurity governance by promoting structured security practices, regulatory compliance, and investment in cybersecurity capabilities. The study also identified implementation challenges, including high compliance costs, shortages of skilled cybersecurity professionals, overlapping regulatory requirements, and the evolving nature of cyber threats. Guided by Institutional Theory, the study demonstrates that regulatory pressures play a crucial role in shaping cybersecurity adoption and enhancing cyber resilience. As digital transformation accelerates, adaptive regulatory approaches and sustained collaboration among regulators, policymakers, and financial institutions will remain essential for maintaining a secure and resilient financial ecosystem in Nigeria.

7. Recommendations

Regulatory authorities should harmonize cybersecurity requirements and strengthen inter-agency collaboration to improve regulatory consistency and reduce compliance complexity. Financial institutions should continue investing in cybersecurity technologies, workforce development, employee awareness, and third-party risk management while integrating cybersecurity into enterprise governance. Continuous regulatory monitoring, stronger enforcement, and enhanced public–private collaboration will further improve cyber resilience, support secure digital transformation, and strengthen the long-term stability of Nigeria's financial sector.

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768555
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

References

Awoleye, O. M., Adebiyi, A. A., & Kolawole, O. J. (2023). Cybersecurity governance and digital transformation in Nigeria's financial sector. *International Journal of Information Security Science, 12*(3), 145–159.

Badamasi, B., & Utulu, S. C. A. (2021). Framework for managing cybercrime risks in Nigerian universities. *arXiv*. https://arxiv.org/abs/2108.09754

Bouveret, A. (2020). *Cyber risk for the financial sector: A framework for quantitative assessment*. International Monetary Fund.

Central Bank of Nigeria. (2022). *Risk-based cybersecurity framework and guidelines for other financial institutions*. Central Bank of Nigeria.

Central Bank of Nigeria. (2023). *Guidelines on information security and cyber resilience for financial institutions*. Central Bank of Nigeria.

Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 (as amended).

European Union Agency for Cybersecurity. (2023). *ENISA threat landscape 2023*. ENISA.

Greitzer, F. L., & Frincke, D. A. (2021). Combating the insider cyber threat. *IEEE Security & Privacy, 19*(1), 61–64.

International Monetary Fund. (2024). *Global financial stability report: Cyber risk and financial stability*. International Monetary Fund.

ISACA. (2023). *State of cybersecurity 2023*. ISACA.

Kshetri, N. (2021). Cybersecurity management in developing economies: Challenges and opportunities. *Journal of Global Information Technology Management, 24*(2), 81–89.

National Information Technology Development Agency. (2019). *Nigeria data protection regulation*. NITDA.

Nigeria Data Protection Act, 2023.

Nigeria Data Protection Commission. (2024). *Guidelines for data controllers and data processors of major importance*. NDPC.

Nigeria Computer Emergency Response Team. (2021). *National cybersecurity policy and strategy 2021*. Office of the National Security Adviser.

Onwubiko, C., & Ouazzane, K. (2022). Multidimensional cybersecurity framework for strategic foresight. *arXiv*. https://arxiv.org/abs/2202.02537

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768555
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Sabo, S. B., & Utulu, S. C. A. (2023). Organization studies based appraisal of institutional propositions in the Nigerian Data Protection Regulation. *arXiv*. https://arxiv.org/abs/2309.12893

Scott, W. R. (2022). *Institutions and organizations: Ideas, interests, and identities* (5th ed.). Sage Publications.

Verizon. (2024). *2024 data breach investigations report*. Verizon Business.

Von Solms, R., & Van Niekerk, J. (2021). From information security to cybersecurity. *Computers & Security, 38*, 97–102.

World Bank. (2022). *Digital development and cybersecurity resilience in emerging economies*. World Bank.

World Economic Forum. (2024). *Global cyber security outlook 2024*. World Economic Forum.