Sociological Research and Innovation (SRI)
Volume 3 Issue 2, Fall 2025
ISSN(P): 3007-3251, ISSN(E): 3007-326X
Homepage: https://journals.umt.edu.pk/index.php/SRI

Check for updates

Title:	**Strategies Adopted by Selected Financial Institutions in Nigeria to Prevent Information Asset Breaches**
Author (s):	Issah Moshood, Tejideen Toyin Olayinka, Lawal Afeez Folorunsho, Araba Toyin Kafayat, Balogun Abdulrauf Oiayinka, and Idowu Samuel Abidemi
Affiliation (s):	University of Ilorin, Ilorin, Nigeria
DOI:	https://doi.org/10.32350/sri.32.05
History:	Received: August 21, 2025, Revised: October 30, 2025, Accepted: November 10, 2025, Published: December 22, 2025
Citation:	Moshood, I., Olayinka, T. T., Folorunsho, L. A., Kafayat, A. T., Oiayinka, B. A., & Abidemi, I. S. (2025). Strategies adopted by selected financial institutions in Nigeria to prevent information asset breaches. *Sociological Research and Innovation*, *3*(2), 82–109. https://doi.org/10.32350/sri.32.05
Copyright:	© The Authors
Licensing:	This article is open access and is distributed under the terms of Creative Commons Attribution 4.0 International License
Conflict of Interest:	Author(s) declared no conflict of interest

A publication of
Department of Sociology, School of Social Sciences and Humanities
University of Management and Technology Lahore, Pakistan

Strategies Adopted by Selected Financial Institutions in Nigeria to Prevent Information Asset Breaches

Issah Moshood[1], Tejideen Toyin Olayinka[1], Lawal Afeez Folorunsho[1*], Araba Toyin Kafayat[2], Balogun Abdulrauf OIayinka[2], and Idowu Samuel Abidemi[2]

[1]Department of Sociology, Faculty of Social Sciences, University of Ilorin, Ilorin, Nigeria
[2]Department of Sociology and Criminology, Faculty of Humanities and Social Sciences, Al-Hikmah University, Ilorin, Nigeria

Abstract

Financial institutions in Nigeria are highly vulnerable to cyber-attacks. Many of them lack the capacity to implement the Central Bank of Nigeria's (CBN) risk-based cybersecurity framework. This has eroded customer trust. Based on the Integrated Systems Theory of Information Security Management, this study aimed to examine strategies adopted by selected financial institutions to prevent information asset breaches. Using a qualitative multiple-case-study approach, data were collected through in-depth interviews with 25 participants (5 Board Members, 5 Senior Managers, 5 Chief Information Security Officers, and 10 IT Officers) from five institutions, supplemented by secondary sources. Thematic analysis revealed that institutions align security plans with organizational strategies and have policies in place, but demonstrate minimal capacity for full CBN compliance. Findings indicate the institutions' 100 percent alignment with internal strategies, but only 40 percent full compliance with CBN's risk-based guidelines based on participant reports. The study recommends CBN-led capacity building to enhance adoption as well as fostering positive social change through restored public confidence.

Keywords: cyber security, information assets, financial institutions, Nigeria, CBN framework, risk management, integrated systems theory

Introduction

The finance sector uses information technology (IT) solutions extensively (Onunka et al., 2023). This use of technology solutions by financial institutions occurs in different forms, i.e., with individual characteristics and consequently varying risk elements (Familoni & Shoetan, 2024). Further, financial breaches have far-reaching implications whenever they occur (Hassan & Ahmed, 2023). The breaches include loss of business,

[*]Corresponding Author: afeezone0606@gmail.com

reputational damage, financial losses owing to an actual loss in the course of the breach or fines, and payment of compensation whenever a breach occurs (Olaniyi et al., 2023). In Nigeria, cybercrime incidents in the financial sector rose by 25% from 2022–2023, resulting in losses exceeding NGN 500 billion (Central Bank of Nigeria, 2015).

It is against this backdrop that financial institutions have formulated strategies to prevent data breaches. These strategies may be used by similar financial services institutions that lack strategies to avoid losses and other consequences of cybercrime (Akintoye et al., 2022). The Nigerian finance sector has evolved significantly in the adoption of technology in service delivery (Hassan et al., 2024). This evolution is in response to the demands of customers who generally have become sophisticated, wanting services at all times, and in specific ways, which technology facilitates (Tarhini et al., 2015). Internet banking, automatic teller machines, mobile banking, fintech services, and other technology-driven service outlets are now a commonplace (Eze et al., 2022).

However, the use of these technologies in finance operations comes with attendant risks (Hinchliffe, 2017). While using these technologies, the institutions can lose money, and they can lose customers and market share if the outcome of technology risk exploitation is not well managed (Chakkaravarthy et al., 2018). It is also common to see that the exploited institutions are fined by regulatory authorities, and in some cases, entire businesses can go closed (Ogunode & Akintoye, 2023). Hence, several finance sector companies in Nigeria have begun to take steps to mitigate the risks that arise from the use of technology for offering services; nevertheless, some do not have corporate strategies which indicates they do not view the issue of preventing cyber exploitation as serious (Hassan et al., 2024). Therefore, this study investigates strategies that have helped players in the sector prevent information security threats and incidents. These strategies can be adopted by other institutions to prevent cybercrime while they use technological tools to provide financial services. While global studies address cybersecurity in financial sectors, limited research explores Nigeria-specific strategies for CBN framework adoption, particularly the interplay of organizational and human factors in preventing breaches.

Purpose of the Study

The purpose of this study is to explore strategies that some financial institutions can use to help prevent cyber exploitations that jeopardize the confidentiality, availability, and integrity of information assets.

Significance of the Study

The significance of the study is that it may help to identify the direction of efforts within IT and cybersecurity to prevent cyber exploitation. It may also provide Chief Information Security Officers (CISOs) with strategies they can adopt to avoid cyber exploitation that may undermine the confidentiality, availability, and integrity of information within the financial sector in Nigeria. Results may also increase the body of knowledge currently available on the subject and extend the applicability and discourse of the Integrated System Theory of information security management. Also, the study may contribute to social change through improved financial inclusion by encouraging increased use of digital finance. Improved confidence in the finance sector may increase the banked population from the current level. In Nigeria, 38.3% of the adult population is currently banked (Central Bank of Nigeria, 2018).

Literature Review

Information Security Policies

Information security policies have been defined as sets of rules guiding the behaviour of IT users to ensure information security in an organisation (Paananen et al., 2020). In other words, policies define acceptable and unacceptable behaviour in the management of information security in an organisation (Niemimaa & Niemimaa, 2017). Also, they determine resources required and how they will be acquired for achieving information security in an organisation. It is the policies that inform the strategies to be formulated and implemented (Ros, 2020). While Paananen et al. (2020) emphasize policy rules for IT behaviour, Niemimaa and Niemimaa (2017) critically highlight their limitations in dynamic Nigerian contexts, where cultural factors may undermine enforcement. This suggests a need for localised adaptations. The study of Stafford et al. (2018) revealed that the policies need to be informed by the business model and organisational objectives of an organisation. In the context of information security, the policies factor in risk identification, assessment, and management as well as all the processes involved.

Internal Controls

Internal controls facilitate the implementation of required technologies, procedures, and policies for detecting and mitigating information security risks. Existing studies indicate that internal control mechanisms are fundamental as they ensure that information security efforts of an organisation are in line with the organisational culture (Sharma & Barua, 2023; Vedral, 2021). Also, studies revealed that internal controls are essential for giving directions on effective ways of handling information security threats and incidents (Kumar, 2023). With internal controls in place, the impacts of information security incidents may be mitigated or future incidents or threats prevented (Rahman & Choo, 2015). Also, internal controls imply information sharing with regulatory bodies or external groups, especially consultants, to reinforce the protection and prevention of information security assets (Sharma & Barua, 2023).

Human Factors in Information Security:

Some studies have emphasized the importance of people in the prevention and management of information assets of organisations (Adelmann et al., 2020; Grandstaff & Solsma, 2021). It is argued that even if an organisation has better technologies and effective internal controls, without supportive people or sound people management, information security breaches would still result (Ghafir et al., 2018). People need to be sensitised and trained on acceptable behaviour necessary for preventing information security breaches. With the proper management of people, human errors that may expose an organisation to information security breaches may be mitigated (Adelmann et al., 2020).

Thus, all stakeholders in the ecosystem of the financial institutions should understand their roles in ensuring the security and integrity of the information assets of an organisation. Both internal and external stakeholders should be made aware of their roles and functions in the management of information assets, as well as policies and procedures they need to follow to prevent information breaches (Grandstaff & Solsma, 2021; Thomaidis, 2022). Human-related risk factors are addressed through organising training and sensitisation programmes for staff (Abraham & Chengalur-Smith, 2019). The study of Hadlington et al. (2019) showed that the intensity and frequency of information security breaches go low when staff are trained and enlightened on processes and procedures for mitigating and preventing information security breaches. These mechanisms may include seminars, talk shops, workshops, email broadcasts, banners, or intranet. This contrasts with global frameworks in Adelmann et al. (2020).

Competence of Information Security Officers

Also, the officers in charge of information management should be knowledgeable in relevant information security management (Adelmann et al., 2020). They should have necessary certifications such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager, and ISO 27001 certification among others. Aside from technical knowledge, they should also have knowledge of business processes connected to the organisation they are protecting or managing its information assets. Other studies revealed that they should have project management knowledge (Familoni & Shoetan, 2024; Hassan et al., 2024). The financial regulatory bodies in Nigeria require that CISOs or IT officers of financial institutions should have CISSP or Certified Information Systems Auditor (Balogun, 2018).

Role of Human Resource Management

Also, studies have pointed out the roles of Human Resource Management (HRM) in ensuring that credible practitioners are employed (Alawonde, 2020; Ogunode & Akintoye, 2023). It is one of the duties of HR to carry out background checks before employing any practitioners because their roles are critical as they deal with information management (Ikusika, 2022). This is essential so that hackers or people of questionable character are not employed. Both background and reference checks are expected to be conducted before hiring (Ololade et al., 2020). To prevent insider threats, it is important to conduct proper checks of the practitioners to be employed (Ojukwu-Ogba & Osode, 2020; Umanhonlen et al., 2020).

One study suggests the importance of checking against a regulatory database before considering and employing new practitioners (Alawonde, 2020). Also, the HR department may sanction any practitioners (staff) that violate information security policies designed to ensure the protection of information assets (Ojukwu-Ogba & Osode, 2020). The sanctions could be extreme, such as dismissal depending on the circumstances and the magnitude of the violation (Umanhonlen et al., 2020). For effective management and protection of information assets, top management is expected to provide necessary resources and frameworks such as ISO 27001 standards (Umanhonlen et al., 2020).

Regulatory Frameworks and Top Management Responsibilities

Studies revealed that organisations need to comply with the regulatory frameworks developed by regulators such as the Central Bank and other key regulators (Ikusika, 2022; Victory et al., 2022). For instance, all cards processed for payments by the financial institutions must be PCI-DSS (Payment Card Industry Data Security Standard) – which requires the deployment of twelve controls certified in Nigeria (Central Bank of Nigeria, 2019; Omotubora & Basu, 2018). Since August 2019, all financial institutions in Nigeria must demonstrate full compliance with the data protection regulation of the National Information Technology Development Agency (NITDA, 2019). Also, existing studies revealed that there is a need for adequate provisions of necessary facilities and resources for the CISO and other IT officers to effectively manage and protect information security of the organisation (Ikusika, 2022; Umanhonlen et al., 2020). The Integrated Systems Theory of Information Security Management (Hong et al., 2003) informs this framework by integrating people, processes, and technology.

Methodology

The study adopted a multiple-case-study design. The purpose of this qualitative multiple case study was to explore strategies deployed to ensure the security of information assets of the selected financial institutions in Lagos, Lagos State, and Abuja, Federal Capital Territory, Nigeria. The population for this study was the Board of Directors (BODs), the Senior Management (SMs), the Chief Information Security Officers (CISOs), and the Information Technology Officers (ITOs) of five selected commercial banks in Nigeria. They were asked about the capacity, readiness, and preparedness of their respective banks to comply with the risk-based cybersecurity framework guidelines for Other Financial Institutions (OFI) developed by the CBN in Nigeria to prevent or mitigate cybersecurity threats and breaches.

The population for this study comprised Board of Directors (BODs) (*n* = 5), Senior Management (SMs) (*n* = 20), Chief Information Security Officers (CISOs) (*n* = 5), and Information Technology Officers (ITOs) (*n* = 40) of five selected commercial banks in Nigeria. From the above, one member from the Board of each financial institution (*n* = 5); one Senior

Management member from each financial institution (n = 5); one CISO from each financial institution (n = 5); and two Information Technology Officers (ITOs) (n = 10). The total sample size for this study was twenty-five (n = 25). Importantly, there is one CISO per financial institution, who is saddled with the responsibility of overseeing cybersecurity policies or guidelines in Nigeria (Balogun, 2018).

The bulk of data for this study was obtained from CISOs that participated in this study. While a census sampling technique was used to select CISOs (because every bank has one CISO), purposive sampling was used to select other participants. For the census sampling technique, the population size is equal to the sample size. Other categories of participants for this study were more than one. Thus, purposive sampling was used to select them. To ensure the validity of the findings, the researchers ensured that data were collected from the right sources. All the participants granted permission for the researchers to use a recording device. So, all the one-on-one interview sessions were recorded and analysed thematically. Additionally, secondary data were also used. The researcher also obtained publicly available documents from the banks' websites and other regulatory websites. The interviews commenced after the ethical approval from the University of Ilorin Ethical Committee. In addition, data triangulation was applied to widen and deepen the understanding of themes emerging from the phenomenon under study.

Data Analysis

Theme 1: Information Security Governance

To understand information security governance, participants were asked questions relating to information security. From the narratives of the participants, the major theme relates to policies, processes, and procedures. All the participants expressed that the framework was not comprehensive as there are some knotty issues in the framework. Participant one expressed that "the framework is not properly communicated to us. There are some issues that are still unclear". All the participants stated that before the formulation of the CBN's framework, they had formulated and implemented policies, processes, and procedures for preventing information security threats.

Table 1

Key Findings

Theme	Key Findings	Board & Senior Management Views	CISO Views	Quantitative Figures	Analysis/Implications
Theme 1: Information Security Governance	Institutions have pre-existing policies, processes, and procedures for information security, integrated into corporate governance. Framework criticized for lack of comprehensiveness and clarity. Board focuses on alignment with business objectives, appointing CISOs, and establishing committees like ISSC.	Board: Emphasize determination to secure customer info, directives for proactivity, policy implementation, alignment with business goals, CISO appointment, and ISSC formation for governance and investment approval (100% of 5 Board members confirmed inclusion in corporate governance). Senior Management: Highlight CISO's importance with qualifications (60% of 5 Senior Management participants), policy formulation based on recommendations, quarterly reporting, and compulsory reading of policies for new staff.	Focus on coordinating security activities, implementing policies, advising board; concerns about lack of support from board/senior management, inadequate resources, and unclear roles (e.g., 20% of 5 CISOs expressed worries about roles not followed); perform risk assessments and backups despite limitations.	- 100% of 25 participants: Framework not comprehensive, pre-existing policies implemented. - 100% of 5 Board members: Included cybersecurity in corporate governance. - 60% of 5 Senior Management: CISO position important. - 20% of 5 CISOs: Board/Senior Management not following roles.	Discrepancy between board/senior management's claimed support and CISOs' reported inadequacies hinders effective risk management. Links to literature: Effective policies crucial for security (Flowerday & Tuyikeze, 2016; Stafford et al., 2018); risk evaluation essential (Hong et al., 2003; Rahman & Choo, 2015; Ismail et al., 2014). In Nigeria, cyberfraud losses reached ₦52.26 billion in 2024, a 195% increase from 2023.
Theme 2: Risk Management Control Functions	Emphasis on addressing threats through policies for assessment, measurement, mitigation, monitoring. Risk treatment options include reduction, avoidance, transfer.	Board: Provide logistics, infrastructures, policies; consider risk management critical (40% of 5 Board members explicitly noted policies for risk processes).	Conduct regular risk assessments, updates for new technologies; options based on assessment results; concerns over lack of support, undefined roles, and ignored reports (60% of 5 CISOs noted lack of	- 100% of 25 participants: Address threats via risk management. - 60% of 5 CISOs: Board/Senior Management not supportive. -	Proper risk identification enables effective mitigation; agrees with literature on risk processes (Akinrolabu et al., 2019; Figueira et al., 2019; Hemanidhi & Chimmanee, 2017). Profiling assets key

Theme	Key Findings	Board & Senior Management Views	CISO Views	Quantitative Figures	Analysis/Implications
	Regular reviews every two years.		support/involvement); identify infrastructure and tools needed.	Reviews: Every 2 years (100% compliance reported by CISOs).	for protection levels. Ransomware in Nigeria's financial sector increased 287% and phishing 178% recently.
Theme 3: Cyber Resilience Assessment	Need to evaluate defense posture, readiness; mandatory by CBN to assess effectiveness of frameworks. Focus on vulnerabilities, threats, impacts on reputation/finances.	Board: Mandate updates on security vulnerabilities/threats, potential impacts; formulate governance frameworks for assessments; evaluate response/recovery capabilities (40% of 5 Board members mentioned mandating updates and frameworks).	View that board/senior management haven't taken major steps (80% of 5 CISOs reported no major steps); difficult to determine losses, recovery time/costs without assessments.	- 80% of 5 CISOs: No major steps by Board/Senior Management. - CBN requires assessment of potential losses (e.g., assets affected, recovery costs/time).	Assessments crucial due to rising breaches; CBN requires info on potential impacts and recovery capabilities to gauge effectiveness. In 2023, 80,658 customers defrauded with ₦17.67 billion losses.
Theme 4: Cybersecurity Operational Resilience	Controls for CIA triad; build resilience through awareness, monitoring, classifications, technologies like DLP, firewalls, antiviruses. Educate staff/external stakeholders on roles.	(Implied support for improvements, but specific views not detailed beyond necessity to improve resilience; ~20% indirect mentions.)	Familiarity with assets, networks, people; monitor info flow, identify unauthorized devices; promote awareness programs, newsletters; implement DLP, document classification, firewalls, database monitoring, antiviruses, endpoint protection; advocate for investments (100% of 5 CISOs reported implementing or advocating tech controls).	- 100% of 5 CISOs: Familiar with assets and implementing controls. - Awareness programs: Monthly newsletters suggested (20% of CISOs).	Resilience aids prompt identification/response; people as key link; complements tech controls with education/sanctions. Early 2023: Three fintechs lost >₦5 billion to hacking.
Theme 5: Cyber-threat Intelligence	Mandate for objective understanding of risks/threats; develop	Board: Deliberating CTI policy formulation and procurement (20% of 5	Need for CTI (80% of 5 CISOs emphasized Board approval needed);	- 80% of 5 CISOs: Board/Senior Management not	Intelligence gathering vital; human elements risky; proactive measures prevent

Theme	Key Findings	Board & Senior Management Views	CISO Views	Quantitative Figures	Analysis/Implications
	CTI policy/program for proactive detection/mitigation. Monitoring stakeholders, access controls, IT changes, endpoint security, micro-segmentation.	Board members mentioned deliberation).	expensive but essential; monitor stakeholders/activities; role-based access, change management, secure endpoints/ports, application templates, micro-segmentation, end-to-end firewalls (100% of CISOs reported monitoring/access controls).	taking CTI seriously. - 100% of 5 CISOs: Implementing monitoring and access controls.	breaches. 2024 bank losses: ₦52.26 billion.
Theme 6: Metrics, Monitoring and Reporting	Mandate for metrics/monitoring of frameworks; demand feedbacks. Disclosure of incidents compulsory to CBN.	Board/Senior Management: Formulated policies; demand feedbacks on effectiveness (20% of 5 Board, 20% of 5 Senior Management mentioned policies/feedbacks).	Ineffective due to limited resources/tools (e.g., no key indicators) (60% of 5 CISOs reported inadequate facilities); prepare reports but poor response; lack clear communication channels, feedbacks; disclosure debated due to dangers, but necessary for learning/prevention (40% agreed with disclosure, 60% disagreed).	- 60% of 5 CISOs: Ineffective metrics due to resources. - 80% of 25 participants: Disclosure challenging but mandatory. - 40% of 5 CISOs: Agreed with disclosure; 60% disagreed.	Monitoring assesses performance; clear channels build synergies; disclosure aids external feedback. 2023 losses: ₦17.67 billion.

Also, all the five selected Board members of each financial institution selected for this study confirmed that they have taken the issue of cybersecurity governance to another level as they have included it in their corporate governance. Participant one expressed that:

> The Board is determined to ensure the security of information of our customers. We have come to understand that information security threats are a major problem that requires serious attention. The Board has given directives to all departments to be more proactive in dealing with information threats, and we have put in place policies and procedures for achieving this.

Similarly, another participant expressed that:

> Information security threats are not a small issue that we can just treat trivially. It is a major concern because of the financial loss, confidence, and reputation loss associated with them. Owing to this, we, at the Board level, have aligned our organisational structure with cybersecurity governance as well as other key and relevant processes. At the Board level, we have prepared strategies, frameworks, and policies required to ensure alignment of cybersecurity with our business goals and objectives, as directed by the CBN's risk-based framework.

Based on the framework, the Board should ensure that information security processes are conducted based on applicable laws and business requirements. One member of the Board added that "the Board is making efforts to establish an Information Security Steering Committee (ISSC) which will consist of senior representatives of relevant departments. The committee will be saddled with the responsibilities for the governance of the information security programme of the organisation". Similarly, another Board participant expressed that "the committee is necessary because of the need to enforce the policies and provide strategic direction for information security governance".

In addition, three out of five Senior Management participants expressed that the position of the CISO is important. But, as shown in the CBN's framework, the person occupying the position should have necessary educational and professional and adequate years of experience in information management and technology. A member of Senior Management expressed that "the board has formulated policies and procedures for ensuring information security based on our recommendations we submitted to them. So, we are ensuring the implementation of those policies here".

Another Senior Management participant expressed that:

> We have information security policies which are guiding and directing our information security risks, incidents, and threats management. We have a document detailing our information security policy. We normally make it compulsory for our new staff, especially IT officers, to read our information security policies.

Also, a CISO expressed that "I understand that my key responsibility is to ensure that information security threats and incidents are mitigated by coordinating the activities of information security within the organisation". Another CISO reported that "I manage the information assets of the organisation based on the decisions of the board. In most cases, I offer advice to the board on what should be done to ensure protection and safety of our information assets". However, one CISO expressed worries that both the Board and Senior Management seem not to have realized their roles in the CBN's framework or have decided not to follow them. According to him:

> Under the new framework, the Senior Management is expected to implement policies, procedures, and processes to protect information [data] of customers as well as transactions. We are in charge of everything. It is my office that is developing a post-incident analysis framework whereas we are supposed to jointly produce it or be given a directive to create it. In addition, it is only my office that is evaluating and managing any risks introduced by third-party service providers. You know there is little we can do without the support of the Board and Senior Management. In my own case, they have not been supportive and serious with the matter of information security. But I'm doing my job in terms of carrying out regular cyber [information risk assessments].

Another CISO participant added that:

> Our Board and Senior Management seem insensitive to information security and management issues. They are only concerned about profits and dividends. They do not know that information security incidents could hamper the profitability of the organisations. I know

> my responsibilities as CISO and I have been discharging them to the best of my ability. My duties include ensuring that the records of users, devices, and applications [and their relationships] are updated regularly.

From the above narratives, there is a discrepancy between board/senior management's claimed support and CISOs' reported inadequacies which hinder effective risk management. All the board members interviewed claimed that cybersecurity is included in corporate governance. 60 percent of the 5 Senior Management members posited that the CISO position is important, while 20 percent of the 5 CISOs mentioned that the Board/Senior Management is not following their roles. However, all the participants claimed that the framework is not comprehensive.

Theme 2: Risk Management Control Functions

To understand risk management control functions in the selected organisations, participants were asked questions relating to risk management control functions. One Board participant said, "at the board level, we consider risk management as a critical activity. We understand that we need to address threats, mitigate exposure, and reduce vulnerability to information security threats. Towards this end, we are providing necessary logistics, infrastructure, and policies". Another Board participant said, "we have formulated policies and processes for effective risk management to aid risk assessment, risk measurement, risk mitigation, and risk monitoring and reporting". One CISO expressed that:

> Processes and controls of information are reviewed every two years in this organisation. I and my team regularly carry out risk assessment, measurement, mitigation, and monitoring and reporting. We are also updating our systems to address new challenges or the introduction or emergence of new technologies. This is necessary because the risk landscape is changing.

Another CISO participant added "we have different risk treatment options depending on the results of the risk assessment. We may decide to adopt options such as risk reduction, risk avoidance, risk transfer, and residual risk". However, three out of five CISOs noted that the Board and Senior Management have not been supportive and adequately involved in the information risk management processes. One CISO participant expressed that:

> They [the Board and the Senior Management] are not providing the necessary logistics, resources, and capabilities to facilitate and ensure adequate and effective risk management. Also, the duties or roles of staff in information risk management are not properly defined. It seems they just put everything on us. What I personally observed is that they don't take our risk reports seriously in terms of providing enabling frameworks, logistics, resources, and capabilities.

Similarly, another CISO participant added:

> I and my team are not relenting in our risk assessment activities. These activities have been helping us to detect and evaluate risks in this organisation. We are also evaluating and analysing whether or not the existing frameworks or programmes for ensuring information security are appropriate and effective. But we have not been gaining much in these areas because of the limited support from top management.

From the foregoing, it can be surmised that proper risk identification enables effective mitigation. All the participants (*n* = 25) agreed that threats can be addressed through risk management. Sixty percent of the five CISOs highlighted that the board/senior management is not supportive. They lamented the lack of support and involvement in identifying infrastructure and tools needed.

Theme 3: Cyber Resilience Assessment

To understand the cyber resilience of the selected institutions, participants were asked questions related to cyber resilience assessment. This was important as it enables the organisation to evaluate its defence posture and readiness to cybersecurity risks. Owing to advances in information and communication technologies, and security threats, the CBN makes it compulsory for the OFIs to carry out resilience assessment to determine the effectiveness of current frameworks for preventing security breaches. A Board participant expressed that:

> We have mandated relevant departments in this organisation to determine and regularly update us about information security vulnerabilities, threats, and the likelihood of their success. Also, we have requested for information on the potential impacts of an exploit

> on the organisation's reputation, financial stability, and regulatory position.

Also, another Board participant gave a note:

> We have formulated effective information security governance frameworks to ensure that we properly carry out vulnerability, incident, and threat assessments. At the Board level, we consider it necessary to know whether we have the capability to swiftly respond to and recover from information security breaches, if they occur.

However, most of the CISO participants were of the view that the Board and Senior Management have not taken any major steps to ensure that they could carry out vulnerability, threat, and incident assessments. Thus, it is difficult to determine the amount of assets and funds that are likely to be lost or the reputation likely to be damaged, and the possibility of recovery if it does happen. The CBN wants to know the capability of OFIs to swiftly respond to and recover from information security threats and incidents.

Theme 4: Cybersecurity Operational Resilience

Also, the study explores cybersecurity operational resilience. To answer this question, the participants were asked about the cybersecurity operational resilience. The CBN directs all OFIs to put in place appropriate control measures to ensure the Confidentiality, Integrity, and Availability (CIA) of their information assets. Most of the Board and Senior Management participants argued that it is necessary to improve their information security resilience. According to a CISO participant:

> With my experience in information systems in this organisation, I'm conversant with the business environment and critical assets. I'm familiar with the software and hardware such as workstations, servers, network devices, and others. Also, I'm conversant with other network devices and internal and external network connections. I can easily identify all unauthorised software and hardware devices on our organisation's network.

Another CISO participant expressed:

> As a Chief Information Security Officer of this organisation, I make sure that I have the identities of all employees and contractors of the organisation. Information flow between us is properly monitored and documented. One of the ways of ensuring information security

> is by being conversant with all the workstations, servers, network devices, and others, as well as people [employees, contractors, and other stakeholders] who communicate with us or with whom we share information.

According to a CISO participant:

> Currently, we have technologies for Data Loss Prevention. If I send a confidential memo through my corporate email to a friend in another organisation, the management will be notified because it bears 'confidentiality'. We can't send out confidential memos to a third party without the knowledge of the management. They will surely know through notifications, and if they know, we are in trouble. Also, to ensure that sensitive documents are treated with utmost care and to avoid information breaches, all documents/files are classified.

A CISO participant was of the view that "We have been persuading the Board and the Senior Management to invest in a firewall solution and Database Activity Monitoring tools necessary to provide maximum security for our applications and to monitor the organisation's databases. Similarly, a CISO participant expressed:

> In this organisation, we have web applications such as firewalls for protecting our applications connected to the Internet [especially unsecured ones] … Also, we have been trying to re-optimise the organisation's network admission and control solution. We have included this in the report we sent to the Board. Hopefully, they would respond to us.

From the above accounts, it is found that resilience aids prompt identification/response. Also, people are a key link, and they complement tech controls with education/sanctions. All the CISOs noted that they were familiar with assets and implementing controls. Also, 20 percent of CISOs suggested monthly newsletters to raise awareness.

Theme 5: Cyber-threat Intelligence

The CBN mandates all OFIs to develop an objective and evidence-based understanding of their information security risks, incidents, and threats. They are expected to have objective knowledge about the causes, effects, and solutions. One Board participant noted that "we are currently deliberating on formulating a Cyber-Threat Intelligence (CTI) policy. So, at the completion of the deliberation, we are likely to procure CTI because we can't afford any information security challenges". Based on the responses of most of the CISO participants, the Board and the Senior Management have not taken it seriously. For instance, one CISO participant gave an account:

> The CBN's framework requires us to establish a Cyber-Threat Intelligence (CTI) programme for proactive identification, detection, and mitigation of potential information security threats and risks. Although I understand it is expensive to procure, it is important because it is useful for mitigating potential information security risks.

Similarly, another CISO participant gave information:

> To aid intelligence-gathering, it is essential for the Board to formulate and approve the CTI policy as it is necessary for proactive identification of emerging information security threats, patterns, trends, risks, and potential impacts. We are likely to get useful information on departments [units] that are vulnerable to threats.

One CISO participant said:

> As a part of intelligence-gathering, we monitor every stakeholder that uses our information. We also monitor those who are monitoring those stakeholders. We checkmate ourselves because people are key elements in information security breaches. Even someone is monitoring me too – my activities on the cyberspace.

From the analysis, 80 percent of the five CISOs mentioned that Board/Senior Management is not taking CTI seriously. Also, all five CISOs expressed that they are implementing monitoring and access controls. Eighty percent of the CISOs emphasized that board approval is required for CTI (Cyber-Threat Intelligence).

Theme 6: Metrics, Monitoring and Reporting

The CBN mandated all financial institutions to ensure that they put in place metrics and monitoring processes for the existing information security framework. One Board participant mentioned that "we have formulated metrics, monitoring and reporting policies based on the strategic objectives of the organisation." Also, a Senior Management participant noted that they normally demand feedback from the CISO and other relevant staff on the effectiveness of existing information security frameworks. However, a CISO participant argued that metrics, monitoring and reporting have not been effective because of limited resources. According to this participant:

> We don't have adequate facilities and resources in this organisation for assessing and evaluating the effectiveness of information security programmes or frameworks. We don't have tools such as key risk indicators, key goal indicators, among others. We don't have all these as the top management is concerned about profits.

In the same vein, another CISO participant mentioned that:

> The Board and the Senior Management have not provided adequate and clear communication channels. This is required for building synergies among relevant departments in the organisation. Since there is no effective communication channel, our information security programmes have not really achieved our targets.

Another CISO participant added:

> It seems the top management is not ready for nipping the information security threats in the bud, going by their dispositions towards it. We are not provided with adequate tools and resources to assess in order to identify the lapses in the existing information security activities and what can be done to improve it. Reporting and communication channels are not clear.

Most of the participants mentioned that disclosure of information security incidents and threats may not be easy, and the CBN makes it compulsory for all OFIs. Based on the framework, OFIs must report incidents of information security breaches, whether successful or not, immediately to the Director of Banking Supervision, Central Bank of Nigeria. While a few CISO participants agreed with this, others disagreed because of its dangers to their organisations. In all, 60 percent of 5 CISOs mentioned that metrics are ineffective due to limited resources. Also, 80 percent of the participants noted that disclosure is challenging; but it is mandatory. While 40 percent of 5 CISOs agreed with disclosure, 60 percent disagreed.

Discussion

The study aims at exploring strategies adopted by financial institutions in

Nigeria to prevent information asset breaches. From the results, it is evident that CBN's framework is unclear to most of the financial institutions. It is argued that to make it work and effective, the CBN needs to make it comprehensive. As noted by Flowerday and Tuyikeze (2016), an effective policy framework is critical for regulating practices and procedures of processing information required for ensuring confidentiality and integrity. Also, Stafford et al. (2018) reported that adhering to policies, processes, and procedures could help in ensuring the security of information assets of firms. Also, the results show that while most of the Board and Senior Management argued that they provide necessary requirements to ensure security of information assets, most of the CISOs argued that they were not getting adequate support from the Board and the Senior Management.

Effective information security management in organisation commences with objective risk evaluation and management (Hong et al., 2003; Rahman & Choo, 2015). Thus, it is critical to conduct risk management because without it the organisation may not know the appropriate strategies to adopt. The analysis implies that the Board and the Senior Management are not adequately directing the CISOs to conduct risk analysis and evaluation, which would inform the strategies, policies, and processes to be adopted.

In addition, the analysis shows that proper risk identification enables effective mitigation. Existing studies revealed that information risk management involves the determination of information security risks, identification of risk tolerance levels of an organisation, and putting in place control mechanisms to mitigate risks (Akinrolabu et al., 2019; Hemanidhi & Chimmanee, 2017). From the results, the importance of risk profiling is established, and this agrees with Hemanidhi and Chimmanee (2017) who showed that it helps to identify the extent and level of protection each information asset needs to ensure their optimum security. In other words, if the risks and threats are identified on time, the organisation through its CISO could quickly mitigate them.

From the results, 60 percent of 5 CISOs mentioned that metrics are ineffective due to limited resources. Also, 80 percent of the participants noted that disclosure is challenging; but it is mandatory. While 40 percent of 5 CISOs agreed with disclosure, 60 percent disagreed. Some studies showed that disclosure of incidents is necessary for others to learn from the experience (Figueira et al., 2019; Hemanidhi & Chimmanee, 2017). The bodies study and assess the nature of the incident and advise others who may be susceptible to it to take precautions or learn how to prevent or mitigate it.

This study contributes to social change through improved financial inclusion by encouraging increased use of digital finance. A significant adult population today in Nigeria does not keep their money in banks due to fear of loss because of a lack of trust in the use of technology. The practice of not keeping cash in banks excludes such people from financial services such as loans and other financial products. Financial inclusion has the potential to provide financial support opportunities to the previously excluded citizens who are unbanked due to information security concerns.

This study contributes to the assurance of possible safe use of finance through technology and may provide opportunities to access funding for previously excluded businesses, which may lead to economic development and other associated benefits from the improved banked population. The study may also help to keep the personal information of customers of financial institutions safe through the deployment of strategies that address threats to information theft, thereby preventing harm and damage through unauthorised access. The implementation of information security strategies identified in the study may allow customers of financial institutions to enjoy better services in an appropriate and more flexible way. Flexible and more convenient finance access will lead to improved customer services. The study may, therefore, help to preserve national heritage and prevent the harm that can impact on national pride and development.

Conclusion

From the analysis, all the participants confirmed that they spend considerable time and effort to inform and train their staff, trading partners, and stakeholders of their roles and responsibilities in keeping their information safe. They also indicated that they have several mechanisms to communicate policies, procedures and processes that guide operations to ensure the safety of information. The participants indicated that the weakest link could be people who are not aware of safe practices in the use of information assets or who, in blind trust, give out information that otherwise should be secret. The participants noted that policies or processes not known can be bypassed, and information security violations can be the result.

Recommendations

Based on the results, the following recommendations are presented

- An organisation should pursue compliance to an identified information security standard related to their business in Nigeria because the need to comply with information security standards was found in the study. When institutions are crafting information security strategies, it is essential to consider regulations requiring compliance in the applicable country.
- Financial institutions in Nigeria need to invest in information security monitoring solutions to stay secure. They should implement solutions that will send alerts if there are potential cyber exploits to address any possible incident. The monitoring should proactively check for the effectiveness of deployed controls to prevent loss due to cyber exploitation.
- Tracking for the effectiveness of controls (policies, processes, and tools) need be deployed to prevent cyber exploitation is vital to stay secure.
- CISOs in organisations should begin to document information security strategies as aligned with the organisational strategy. Enterprise risk managers should start demanding from CISOs a documented strategy for information security risk management.

Conflict of Interest

The authors of the manuscript have no financial or non-financial conflict of interest in the subject matter or materials discussed in this manuscript.

Data Availability Statement

Data supporting the findings of this study will be made available by the corresponding author upon request.

Funding Details

No funding has been received for this research.

Generative AI Disclosure Statement

The authors did not used any type of generative artificial intelligence software for this research.

References

Abraham, S., & Chengalur-Smith, I. (2019). Evaluating the effectiveness of learner-controlled information security training. *Computers & Security, 87*, Article e101586. https://doi.org/10.1016/j.cose.2019.101586

Adelmann, F., Ergen, I., Gaidosch, T., Jenkinson, N., Khiaonarong, M. T., Morozova, A., Wilson, C. (2020). *Cyber risk and financial stability: It's a small world after all*. International Monetary Fund.

Akinrolabu, O., Nurse, J., Martin, A., & New, S. (2019). Cyber risk assessment in cloud provider environments: Current models and future needs. *Computers & Security, 87*, Article e101600. https://doi.org/10.1016/j.cose.2019.101600

Akintoye, R., Ogunode, O., Ajayi, M., & Joshua, A. A. (2022). Cyber security and financial innovation of selected deposit money banks in Nigeria. *Universal Journal of Accounting and Finance, 10*(3), 643–652.

Alawonde, K. O. (2020). *Tailored information security strategies for financial services companies in Nigeria* [Doctoral dissertation, Walden University]. Scholarworks. https://scholarworks.waldenu.edu/dissertations/8662/

Balogun, K. O. (2018). *Letter to all banks and payment service providers: Exposure draft of the risk-based cybersecurity framework and guidelines for deposit money banks and payment service providers*. Central Bank of Nigeria.

Central Bank of Nigeria. (2015). *Regulatory and supervisory guidelines for development finance institutions in Nigeria*. https://www.cbn.gov.ng/out/2015/ofisd/regulatory%20and%20supervisory%20guidelines%20for%20development%20finance%20institutions%20in%20nigeria%202015.pdf

Central Bank of Nigeria. (2018). *National financial inclusion strategy (Revised)*. https://www.cbn.gov.ng/out/2019/ccd/national%20financial%20inclusion%20strategy.pdf

Central Bank of Nigeria. (2019). *Nigeria financial services industry IT standards blueprint*. https://www.cbn.gov.ng/itstandards/IT_Standards_Blueprint_V1.0.pdf

Chakkaravarthy, S., Sangeetha, D., Venkata Rathnam, M., Srinithi, K., & Vaidehi, V. (2018). Futuristic cyber-attacks. *International Journal of Knowledge-Based Intelligent Engineering Systems, 22*(3), 195–204. https://doi.org/10.3233/KES-180384

Eze, C. U., Ebe, E. C., Okwo, I. M., Ibeabuchi-Ani, O., Odume, M. S., Godspower, J. O., & Obeagu, E. I. (2022). Effect of the capability component of fraud theory on fraud risk management in Nigerian banks. *International Journal of Financial Research*, *13*(1), 90–95.

Familoni, B. T., & Shoetan, P. O. (2024). Cybersecurity in the financial sector: A comparative analysis of the USA and Nigeria. *Computer Science & IT Research Journal*, *5*(4), 850–877.

Figueira, P. T., Bravo, C. L., & López, J. R. (2019). Improving information security risk analysis by including threat-occurrence predictive models. *Computers & Security*, *88*, Article e101609. https://doi.org/10.1016/j.cose.2019.101609

Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers & Security*, *61*, 169–183. https://doi.org/10.1016/j.cose.2016.06.002

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., & Baker, T. (2018). Security threats to critical infrastructure: The human factor. *The Journal of Supercomputing*, *74*(10), 4986–5002. https://doi.org/10.1007/s11227-018-2337-2

Grandstaff, J. L., & Solsma, L. L. (2021). Financial statement fraud: A review from the era surrounding the financial crisis. *Journal of Forensic and Investigative Accounting*, *13*(3), 421–437.

Hadlington, L., Popovac, M., Janicke, H., Yevseyeva, I., & Jones, K. (2019). Exploring the role of work identity and work locus of control in information security awareness. *Computers & Security*, *81*, 41–48. https://doi.org/10.1016/j.cose.2018.10.006

Hassan, A. O., Ewuga, S. K., Abdul, A. A., Abrahams, T. O., Oladeinde, M., & Dawodu, S. O. (2024). Cybersecurity in banking: A global perspective with a focus on Nigerian practices. *Computer Science & IT Research Journal*, *5*(1), 41–59.

Hassan, A., & Ahmed, K. (2023). Cybersecurity's impact on customer experience: An analysis of data breaches and trust erosion. *Emerging Trends in Machine Intelligence and Big Data*, *15*(9), 1–19.

Hemanidhi, A., & Chimmanee, S. (2017). Military-based cyber risk assessment framework for supporting cyber warfare in Thailand. *Journal of Information & Communication Technology*, *16*(2), 192–222.

Hinchliffe, A. (2017). Nigerian princes to kings of malware: The next evolution in Nigerian cybercrime. *Computer Fraud & Security*, *2017*(5), 5–9. https://doi.org/10.1016/S1361-3723(17)30040-4

Hong, K., Chi, Y., Chao, L., & Tang, J. (2003). An integrated system theory of information security management. *Information Management & Computer Security*, *11*(5), 243–248. https://doi.org/10.1108/09685220310500153

Ikusika, B. (2022). *A critical analysis of cybersecurity in Nigeria and the incidents of cyber-attacks on businesses/companies*. Social Science Network. https://ssrn.com/abstract=4165204

Ismail, S., Sitnikova, E., & Slay, J. (2014). *Using integrated system theory approach to assess security for SCADA systems cybersecurity for critical infrastructures* [Paper presentation]. Proceedings of 2014 11th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), Xiamen, China.

Kumar, I. (2023). Emerging threats in cybersecurity: A review article. *International Journal of Applied and Natural Sciences*, *1*(1), 01–08.

National Information Technology Development Agency. (2019). *Nigeria data protection regulation*. https://nitda.gov.ng/wp-content/uploads/2019/01/NigeriaDataProtectionRegulation.pdf

Niemimaa, E., & Niemimaa, M. (2017). Information systems security policy implementation in practice: From best practices to situated practices. *European Journal of Information Systems*, *26*(1), 1–20. https://doi.org/10.1057/s41303-016-0025-y

Ogunode, O. A., & Akintoye, R. I. (2023). Financial technologies and financial inclusion in emerging economies: Perspectives from Nigeria. *Asian Journal of Economics, Business and Accounting*, *23*(1), 38–54.

Ojukwu-Ogba, N., & Osode, P. C. (2020). The legal combat of financial crimes: A comparative assessment of the enforcement regimes in Nigeria and South Africa. *African Journal of Legal Studies*, *13*(2), 130–152.

Olaniyi, O. O., Olaoye, O. O., & Okunleye, O. J. (2023). Effects of information governance (IG) on profitability in the Nigerian banking sector. *Asian Journal of Economics, Business and Accounting*, *23*(18), 22–35.

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

Omotubora, A., & Basu, S. (2018). Regulation for e-payment systems: Analytical approaches beyond private ordering. *Journal of African Law*, *62*(2), 281–313. https://doi.org/10.1017/S0021855318000104

Onunka, O., Alabi, A. M., Okafor, C. M., Obiki-Osafiele, A. N., Onunka, T., & Daraojimba, C. (2023). Cybersecurity in US and Nigeria banking and financial institutions: review and assessing risks and economic impacts. *Advances in Management*, *1*(2), 54–62.

Paananen, H., Lapke, M., & Siponen, M. (2020). State of the art in information security policy development. *Computers & Security*, *88*, Article e101608. https://doi.org/10.1016/j.cose.2019.101608

Rahman, N. A., & Choo, K. (2015). A survey of information security incident handling in the cloud. *Computers & Security*, *49*, 45–69. https://doi.org/10.1016/j.cose.2014.11.006

Ros, G. (2020). *The making of a cyber crash: A conceptual model for systemic risk in the financial sector*. ESRB Occasional Paper Series.

Sharma, P., & Barua, S. (2023). From data breach to data shield: The crucial role of big data analytics in modern cybersecurity strategies. *International Journal of Information and Cybersecurity*, *7*(9), 31–59.

Stafford, T., Deitz, G., & Li, Y. (2018). The role of internal audit and user training in information security policy compliance. *Managerial Auditing Journal*, *33*(4), 410–424. https://doi.org/10.1108/MAJ-07-2017-1596

Tarhini, A., Mgbemena, C., Trab, M., & Masa'deh, R. (2015). User adoption of online banking in Nigeria: A qualitative study. *Journal of Internet Banking and Commerce*, *20*(132), 1–24.

Thomaidis, A. (2022). Data breaches in hotel sector according to General Data Protection Regulation (EU 2016/679). In M. Valeri (Ed.), *Tourism* *risk: Crisis and recovery management* (pp. 129–140). Emerald Publishing Limited.

Umanhonlen, F. O., Otakefe, J. P., & Osikhenaogiedu, K. (2020). Combating economic and financial crimes in Nigeria: The role of the forensic accountant. *Journal of Management and Science*, *10*(4), 12–28.

Vedral, B. (2021). *The vulnerability of the financial system to a systemic cyberattack* [Paper presentation]. Proceedings of the 13th International Conference on Cyber Conflict (CyCon). Tallinn, Estonia.

Victory, C. O., Promise, E., & Mike, C. N. (2022). Impact of cybersecurity on fraud prevention in Nigerian commercial banks. *Jurnal Akuntansi, Keuangan, dan Manajemen*, *4*(1), 15–27.