ISLAMIC UNIVERSITY JOURNAL OF SOCIAL SCIENCES VOL 4, NO 6

ISSN: 2709-2429(Print), 2709-2437(Online)-Published 31st December 2025

Strategies Adopted By Selected Financial Institutions In Nigeria To Prevent Information Asset Breaches

by

ISSAH Moshood; TEJIDEEN Toyin Olayinka; LAWAL Afeez Folorunsho; ARABA Toyin Kafayat; BALOGUN Abdulrauf OIayinka; IDOWU Samuel Abidemi

[1,2,6]Department of Sociology, Faculty of Social Sciences, University of Ilorin, Ilorin, Nigeria.

[*3,4,5]Department of Sociology and Criminology, Faculty of Humanities and Social Sciences, Al-Hikmah University, Ilorin, Nigeria.
*Corresponding Author: **afeezone0606@gmail.com**

Abstract

Financial institutions in Nigeria face high vulnerability 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 show minimal capacity for full CBN compliance. Findings indicate 100 per cent alignment with internal strategies, but only 40 per cent 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: Cybersecurity, Information Assets, Financial Institutions, Nigeria, CBN Framework, Risk Management, Integrated Systems Theory.

Research Problem

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

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 commonplace (Eze et al., 2022).

However, the use of these technologies in finance operations comes with attendant risks (Hinchliffe, 2017). 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 exploited institutions fined by regulatory authorities, and in some cases, entire businesses can close (Ogunode & Akintoye, 2023). It is, therefore, important for financial institutions to take the issue of preventing cyber exploitation seriously (Eze et al., 2022). 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 that indicate they view the issue of preventing cyber exploitation as serious (Hassan et al., 2024). Therefore, the study investigated strategies that have helped players in the sector prevent information security threats and incidents, which other institutions can adopt to prevent cybercrime in the **use** of 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 organisational and human factors in preventing breaches.

Purpose of the Study

The purpose of this study is to explore strategies some financial institutions use to 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 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 IST theory of information security management. Also, the study may help contribute to social change through improved financial inclusion by encouraging increased use of digital finance. Financial inclusion has the potential to provide financial support opportunities to previously excluded citizens who are unbanked due to information security concerns about saving money in financial institutions in Nigeria. 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). The assurance of the safe use of financial services through technology can provide opportunities to access funding for businesses, which may lead to economic development and other associated benefits from the improved banked population (Ngwu, 2014). Digital finance stimulates growth, which in turn leads to improved gross domestic product (GDP) in developing economies (Ozili, 2018).

Literature Review

The review is done based on the following sub-headings:

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. As noted by Niemimaa and Niemimaa (2017), policy determines and directs technologies and processes required for ensuring the protection of information assets. To achieve the security of information assets, there must be comprehensive policies in place to cater for all potential information security risks. 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. Hong et al.(2003) argued that security policies are critical for ensuring effective information security management. Similarly, Leung et al. (2015) noted that information security policies exist to ensure the safety and protection of information assets of an organisation. Also, for effective and adequate internal controls for managing information security, relevant policies need to be in place to guide acceptable use of technology (Labrecque et al., 2021). In addition, they ensure the effective deployment and use of technologies. In addition, policies assist in determining when and where lapses or violations occur during the monitoring stage of information security (Nish et al., 2022).

Internal Controls:

There are studies on internal controls (Rae et al., 2017; Labrecque et al., 2021). It is argued that 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 (Labrecque et al., 2021; Kumar, 2023). With internal controls in place, the impacts of information security incidents may be mitigated or future incidents or threats prevented (Ab Rahman & Choo, 2015). Also, internal controls imply information sharing with regulatory bodies or external groups, especially consultants, to aid 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 (Grandstaff & Solsma, 2021; Adelmann et al., 2020). 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. There are certain behaviours that people need to exhibit in an organisation to prevent information breaches (Bauer et al., 2017). To manage people in the context of information security, training and sanctions could be applied. With the proper management of people, human errors that may expose an organisation to information security breaches may be mitigated (Adelmann et al., 2020).

All staff and other stakeholders should be made aware of their roles in the information security chain. In other words, 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. Studies revealed that 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 (Thomaidis, 2022; Grandstaff & Solsma, 2021). They need to understand these policies, procedures, and processes because if they do not understand, there may not be progress in the fight against information breaches (Torten et al., 2018).

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 reduced when staff are trained and enlightened on processes and procedures for mitigating and preventing information security breaches. The authors added that the human factor in information security management is critical in achieving the safety and security of information assets. Mechanisms for creating awareness among staff should be put in place. These mechanisms may include seminars, talk shops, workshops, email broadcasts, banners, or intranet. In Nigeria, studies like Ikusika (2022) reveal underexplored gaps in local cyber-attack responses. This contrasts with global frameworks in Adelmann et al. (2020). Diesch et al.(2020) found that both technological and human factors are fundamental in the management of information assets.

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). Also, 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). Existing studies revealed that if knowledgeable and skilful information security practitioners are employed, errors during the configuration, formulation, and implementation of information security policies and controls will be reduced (Ikusika, 2022; Ololade et al., 2020). This implies that employing and engaging skilled personnel is one step in risk management (Haqaf & Koyuncu, 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 (Ogunode & Akintoye, 2023; Alawonde, 2020). 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). Studies revealed that to prevent insider threats, it is important to conduct proper checks of the practitioners to be employed (Umanhonlen et al., 2020; Ojukwu-Ogba & Osode, 2020). One study suggests the importance of checking against a regulatory database before considering and employing new practitioners (Alawonde, 2020). In the database, there are names of various practitioners of different organisations that have exited their organisations because they were involved in one fraudulent activity or another (Ogunode & Akintoye, 2023).

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). Some staff members that violate the

policies may go through disciplinary actions. If the violation is made a punishable offence, the level of violation is likely to be minimal (Ali et al., 2017). Studies have shown the importance of the Board and the Senior Management in the management of information security (Andress & Leary, 2017; Meriah & Arfa Rabai, 2019; Lanz, 2017). 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). Also, it is the responsibility of top management to provide internal controls necessary for protecting information assets of an organisation (Alawonde, 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 (Victory et al., 2022; Ikusika, 2022). For instance, all cards processed for payments by the financial institutions must be PCI-DSS (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). It is argued that the required IT tools should be provided for IT practitioners in an organisation. The nature of IT tools provided by top management and used by the CISO determines the effectiveness of information risk management in an organisation (Han et al., 2016; Rasekh et al., 2016). To secure the information assets of an organisation, relevant technologies must be provided by top management as suggested by information security practitioners (de Gusmão et al., 2016). The Integrated Systems Theory of Information Security Management (Hong et al., 2003) informs this framework by integrating people, processes, and technology. In Nigeria, this theory underscores the need for holistic strategies, as isolated policies (Familoni & Shoetan, 2024) fail without human training and regulatory alignment.

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).

They are responsible for protecting the information assets of their institutions (Karanja, 2017). They have the competence and expertise to design and implement strategies or procedures for preventing or mitigating cyber threats or breaches in their institution (Reece & Stahl, 2015). Their major responsibility is to ensure the information security of their organisation (Hooper & McKissack, 2016). 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. In other words, those that met the eligibility criteria participated in the study. Some interviews

were conducted on a one-on-one basis in the participants' offices; others were conducted through emails or phone conversations.

All the participants granted permission for the researchers to use a recording device. So, all the one-on-one interview sessions were recorded. After the initial interviews, each interviewee was contacted again to confirm that what they expressed was adequately and correctly captured. This is known as member checking (Madill & Sullivan, 2018) as mentioned earlier. The recorded interviews were transcribed and summarised clearly and concisely to ensure that all the major points expressed by the interviewees were included. The summarised points were sent to the interviewees for confirmation: if they represent or reflect their views and opinions during the interview. Wrong information was corrected as detected. Additionally, secondary data were also used. During the interviews, some participants provided the researcher with some important documents which were read and analysed. The researcher also obtained publicly available documents from the banks' websites and other regulatory websites. The researchers reviewed the banks' websites before and after the interview sessions. According to Yin (2013), additional sources of data have the potential to increase the validity and reliability of studies. The interviews commenced after the ethical approval from the University of Ilorin Ethical Committee.

To get the participants, relevant executive-level officers such as executive directors of the selected banks provided the researchers with information regarding organisational procedures and approvals to gain access to the participants. These executive officers enabled the researchers to have contact with the gatekeepers, and the gatekeepers gave formal approval to have access to the participants. Access was facilitated through professional networks and gatekeepers in the institutions. They helped the researcher to contact participants based on their existing relationships as neighbours and friends. They directed the gatekeepers or designated representatives to notify the participants to participate in the study, and they instructed them to share information required from them without any fear. The gatekeeper made the research process smooth and effective as they gave the researchers the e-mail and phone details of the participants.

Initially, the participants were contacted via emails where permissions were sought to call them on the phone, which most of them granted. The letter of consent to participate was also sent via

email. In this email, the details of the study were provided, and rapport began to develop. After the email, those who replied that the researcher should call them on the phone were called, and the place and timing of the interviews were decided. They were assured of the anonymity of the outcome of the research. Through the researcher's contact in one of the selected banks, he got contacts of other banks from him, and the same processes and procedures were strictly followed. Other categories of participants were included because of their roles in the implementation of the risk-based cyber-security framework guidelines for Other Financial Institutions (OFI) developed by the CBN in Nigeria. The selected commercial banks are bound by the risk-based cyber-security framework guidelines for Other Financial Institutions (OFI), and the full implementation must be done by 1st January 2023.

Data triangulation was applied to widen and deepen the understanding of themes emerging from the phenomenon under study. Kern (2016) argued that data triangulation allows researchers to use at least two data collection methods to investigate a phenomenon. Multiple data sources helped reduce biases that may have arisen. This is because through the use of multiple data sources, there would be convergence or divergence of data. The non-textual data such as audio files were transcribed. It was necessary to convert the data because they were in recording form. Thus, they were transcribed from audio to text. To prevent a mix-up, five electronic folders were used to store data for each financial institution for this study. Interview audio files and the transcribed versions, as well as soft copies of secondary data, were stored in separate folders for each of the selected banks. Importantly, themes were derived using thematic analysis: initial open coding of transcripts identified patterns, followed by axial coding to group them into categories (such as governance, risk management), guided by the Integrated Systems Theory.

Ethical Consideration

After the participants had agreed to participate in the study, the researchers contacted the participants via e-mail, and the letter of consent was attached to the emails sent to all the prospective participants. The participants completed and returned the letter of consent before scheduling the interview sessions. They consented to be part of this study, and this revealed that their rights as participants were well acknowledged and preserved (Hammer, 2016). By willingly completing and returning the letter of consent, it means that they were showing willingness to

participate in the study. Also, ethical approval was obtained from the University of Ilorin Ethical Committee. The participants were told that they could withdraw from this study via telephone call, formal written letter, or e-mail. No monetary incentive was provided or given to the participants for agreeing to or participating in this study. The selected commercial banks were promised through a formal letter that they would get a copy of the research reports in case they might benefit from it. The identities of the participants were not revealed as their names and their institutions were not mentioned (Saunders et al., 2015). This is necessary to ensure the confidentiality of their opinions and experiences, as well as information of their banks. The data obtained were stored in a Google Drive inside a folder created for this study for a period of one year. Google authentication and encryption protocols were used to secure the folder.

Data Presentation and Analysis

In this section, data were presented and analysed. It should be noted that 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. As mentioned earlier, the population for this study comprised Board Members, Senior Management Officials from each financial institution, CISOs from each financial institution, and Information Technology Officers (ITOs). 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 results are presented in themes as follows:

Table 1: Key Findings

Theme	Key Findings	Board & Senior Management Views	CISO Views	Quantitative Figures	Analysis/Implications
Theme 1: Information	Institutions have pre-existing	Board: Emphasize determination	Focus on coordinating security	- 100% of 25 participant	Discrepancy between board/senior

Security Governance	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.	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.	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.	s: 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.	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; Ab 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	Emphasis on addressing threats through	Board: Provide logistics, infrastructures, policies;	Conduct regular risk assessments, updates for new	- 100% of 25 participants: Address	Proper risk identification enables effective mitigation;

Control Functions	policies for assessment, measurement, mitigation, monitoring. Risk treatment options include reduction, avoidance, transfer. Regular reviews every two years.	consider risk management critical (40% of 5 Board members explicitly noted policies for risk processes).	technologies; options based on assessment results; concerns over lack of support, undefined roles, and ignored reports (60% of 5 CISOs noted lack of support/involvement); identify infrastructure and tools needed.	threats via risk management. - 60% of 5 CISOs: Board/Senior Management not supportive. - Reviews: Every 2 years (100% compliance reported by CISOs).	agrees with literature on risk processes (Akinrolabu et al., 2019; Hemanidhi & Chimmanee, 2017; Inskeep, 2019; Ionescu et al., 2019; Tubío Figueira et al., 2019). Profiling assets key 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	Controls for CIA triad; build resilience through	(Implied support for improvements, but specific views not	Familiarity with assets, networks, people; monitor info flow,	- 100% of 5 CISOs: Familiar with assets and	Resilience aids prompt identification/response; people as key link;

Resilience	awareness, monitoring, classifications, technologies like DLP, firewalls, antiviruses. Educate staff/external stakeholders on roles.	detailed beyond necessity to improve resilience; ~20% indirect mentions.)	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).	implementing controls. - Awareness programs: Monthly newsletters suggested (20% of CISOs).	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 CTI policy/program for proactive detection/mitigation. Monitoring stakeholders, access controls, IT changes, endpoint security, micro-segmentation.	Board: Deliberating CTI policy formulation and procurement (20% of 5 Board members mentioned deliberation).	Need for CTI (80% of 5 CISOs emphasized Board approval needed); 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	- 80% of 5 CISOs: Board/Senior Management not taking CTI seriously. - 100% of 5 CISOs: Implementing monitoring and access controls.	Intelligence gathering vital; human elements risky; proactive measures prevent breaches. 2024 bank losses: ₦52.26 billion.

			reported monitoring/access controls).		
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 (Wagner et al., 2019). 2023 losses: ₦17.67 billion.

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. 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. We are also assigning responsibilities to relevant offices, especially the Senior Management. Also, we review reports from them on information security programmes they have embarked on. In short, we quickly approve programmes submitted by the Senior Management aimed at achieving cyber safety and security.

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. Due to this, we, at the board level, have aligned our organisational structure with cybersecurity governance as well as other key and relevant processes. We are doing what we are supposed to be doing within the limits of existing legislation (Member of the Board). 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, we have appointed a qualified person to oversee and implement our cybersecurity programmes. This person is called CISO [Chief Information Security Officer].

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 … In addition, it will ensure that information security policies and processes are aligned with the organisation's business objectives. Also, it evaluates, approves, and sponsors organisation-wide information security investments". Similarly, another Board participant expressed that "the committee is necessary because of the need to enforce the implementation of policies and standards on information security as well as to 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 acquiring the position should have necessary educational and professional qualifications such as a Masters in Cyber or Information Security, Certified Information Systems Security Professional (CISSP), and

Certified Information Security Manager (CISM). Also, he/she must have had adequate years of experience in information management and technology.

In addition, 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 member of Senior Management noted that "we will make it a tradition henceforth to submit reports to the board on information security programmes of our organisation on a quarterly basis. We did this before, but not on a quarterly basis. We want to start now because of the seriousness of the threats in recent times". One 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. These policies have informed our strategies and procedures.

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 noted that "I manage the information assets of the organisation based on the decisions of the board. Also, I ensure the implementation of information security policies and standards 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". In addition, "I need to make it clear to you that my position is different from that of the Head of Information Technology (IT). I am not mandated to report to them because we are independent, though we work together to ensure the security and safety of our information assets."

However, one CISO expressed worries that both the Board and Senior Management seem not to have understood 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. From their actions so far, I can rightly say that they think information security issues are not important. We can't be effective if the Senior Management and the Board are not providing enabling facilities and the policy framework required. But I'm doing my job in terms of carrying out regular cyber [information risk assessments]. We are also conducting frequent data backups of critical IT systems to a separate storage location.

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 because they are associated with huge financial and reputation losses. 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. Also, I'm expected to manage software and hardware asset inventory as well as the utilisation of network and data performance in this organisation. I and my team have been carrying this out with limited support from top management.

Also, a CISO participant noted that:

> I have been helping this organisation to formulate and implement information security strategies and planning. I'm just trying because the organisation has not been responsive in terms of providing necessary resources and capabilities to make my goals achievable. Assuming the top management and the board provide all the needed resources, we would have developed better techniques and methodologies for identifying and mitigating information security threats and incidents.

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. Sixty per cent of the 5 Senior Management members posited that the CISO position is important, while 20 per cent 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 noted that "at the board level, we consider risk management as critical. 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 that "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. We formulate a risk management programme based on our understanding of threats and vulnerabilities, the risk profile, and the level of risk tolerance of the organisation.

Another CISO participant added that "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. Also, one of the roles is to report the information we obtained through risk management activities to Senior Management as well as the Board of Directors for policy formulation and decision-making. 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 that:

> I and my team are not relenting in our risk assessment activities such as assessing vulnerability and threat analysis. 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 achieving much in these areas because of the limited support from top management.

One CISO participant noted that:

> We normally prepare and deliver an information security risk management report to the board regularly even though they don't usually respond, not to talk of doing the necessary things … one of my duties as a CISO is to identify information security risks on a daily basis. As a CISO, I understand that I must have expertise in identifying IT infrastructure in my environment as well as the right tools to use to address specific information security risks.

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 per cent of the five CISOs stressed 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 is necessary and important as it enables the organisation to evaluate its defence posture and readiness to cybersecurity risks. Due to advances in information and communication technologies and their adoption in most organisations, especially in the financial sector, the incidents of information security breaches have grown significantly in recent times. Therefore, the CBN makes it compulsory for the OFIs to carry out resilience assessment in order to determine the effectiveness of current frameworks and processes for preventing and mitigating information security incidents. A Board participant expressed that:

> We have mandated relevant departments in this organisation to determine and regularly update us with information about information security vulnerabilities, threats, and potential incidents and the likelihood of their success. Also, we instruct them to furnish us with the information on the potential impacts of an exploit on the organisation's reputation, financial stability, and regulatory position.

Also, another Board participant noted that:

> 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. We also need to know whether the existing frameworks, programmes, policies, and processes are effective or not.

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 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 if the incident occurs, and the possibility of recovery if it does happen, as well as the recovery time or what is required to recover. The CBN demands information about the likely amount of assets that would be affected if an information security incident occurs, as well as how much is required and what time is needed for the organisation to recover from losses or damages associated with potential cyber incidents. The CBN wants to know the capability of OFIs to swiftly respond to and recover from information security threats and incidents. Also, it wants to know whether the existing frameworks and procedures are effective in identifying, controlling, and mitigating risks. In all, assessments are crucial due to rising breaches. Also, the CBN requires information on potential impacts and recovery capabilities to gauge effectiveness.

Theme 4: Cybersecurity Operational Resilience

Also, the study explores cybersecurity operational resilience. To answer this question, the participants were asked questions relating to 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. If I

> discover, or my team discovers, them, I normally take actions such as identifying, documenting, removing, or reporting them.

Another CISO participant expressed that:

> 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.

Also, another participant added that:

> My team has been helping this organisation to build information security resilience. We understand that this is fundamental because customer information and other relevant information are key assets of the organisation, and we must do everything to protect them. Developing information security resilience will help in prompt identification of information security vulnerabilities, threats, and related risks. This will enable us to develop swift and rapid information security incident response.

A CISO participant expressed that:

> We need to let all the staff understand their functions and roles in the information security chain. We have technology controls, policies, strategies, and processes in place. But, to make them work, we need to educate people on them. Without understanding, nothing meaningful can be achieved. There is the need for a regular security awareness programme. A newsletter should be shared and circulated every month where critical issues relating to information security are discussed. We complement this with other awareness programmes. With what we are doing, I think the staff members are aware of their expectations and they know that if they do not meet those expectations, there would be consequences [information security breaches]; and they don't want the consequences.

Another CISO added that:

> Staff members need to be aware of the guidelines. They need to be informed of the implications of their activities in the organisation. They need to be told what behaviours are expected of them in the fight against information security breaches. Also, external stakeholders [those who interact with their IT infrastructure] also need to be aware of the policies, procedures, and processes of information security management.

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 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 necessary to provide maximum security for our applications … Also, we have been advising the Senior Management to provide Database Activity Monitoring tools that we can use to monitor activities of authorised and unauthorised people on the organisation's databases … Besides this, we have procured antivirus software that we use to scan the system. This is necessary to remove viruses in the system. We also have end-user devices for protecting our information assets". Similarly, a CISO participant expressed that:

> 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. If we are able to get it, unauthorised connections will be easily detected. Any connection must be approved by the central unit.

From the above narratives, 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 per cent 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. This means that they need to constantly conduct research about information security incidents and threats to protect the information assets of the organisation. 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 expressed that:

> 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 in terms of procurement and maintenance, it is important because it is useful for detecting and mitigating potential information security risks.

Similarly, another CISO participant noted that:

> 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 and susceptible to threats and risks.

One CISO participant expressed that:

> As part of intelligence-gathering, we monitor every stakeholder that uses our information. We also monitor those that 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 and that. When it comes to information security, you don't trust anyone. Any staff can be compromised either deliberately or unknowingly. When I say monitoring, I mean we are monitoring their activities in cyberspace. For instance, we monitor their connections to internal and external computers as well as their devices.

Another CISO participant expressed that:

> As a way of ensuring information security, there is a process in place that assigns access by roles. A CISO participant expressed that "each staff member is assigned specific roles. We give each IT and non-IT staff member specific access to their job specification. The access given to a specific staff member is limited to their role. Also, we have a functioning and effective IT change management process. We have configured our IT to the extent that no staff or third party that is not authorised can change our IT infrastructure. This helps to prevent unauthorised changes in our critical information management and security infrastructure. We also have mechanisms and processes in this organisation for hardening and securing endpoints which have connections with IT infrastructure.

A CISO participant expressed that:

> We identify and configure our devices through the endpoints that connect to our infrastructure. This is necessary because the IT platforms are highly sensitive. Also, all the ports that are not necessary are locked down; we only connect our system to the organisation-owned system. Having many ports may be risky and make us susceptible to attacks … We also have application deployment templates which we developed through our IT officers. It is these templates that are given to our developers to guide their coding methodologies in building information security into applications.

Another CISO participant expressed that:

> To ensure security of information assets, we are trying to see how we can use micro-segmentation within local area networks for managing and controlling what our endpoints connect to. We need to manage our ecosystem because hackers may use any loopholes to penetrate. Also, my firewall is here and I ensure that it is end-to-end. To prevent malware, we do micro-segmentation. By this, systems in the same office [room] cannot interact or connect to each other unless we reconfigure them to do so. Another thing we do is that we make sure that we have an application security baseline document detailing security measures that should be incorporated or configured during web- and mobile-app development.

From the analysis, 80 per cent 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 per cent of the CISOs emphasised 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 expressed that "we have formulated metrics, monitoring and reporting policies based on the strategic objectives of the organisation." Also, a Senior Management participant noted that we normally demand feedback from the CISO and other relevant staff on the effectiveness of existing information security frameworks. A CISO participant argued that metrics, monitoring and reporting have not been effective because of limited resources. According to a CISO 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 need to assess the performance and effectiveness regularly. 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 not concerned about profits without taking care of those things that may affect the capability of the organisation to make a profit. We are doing what we can within the limits of our power by preparing and providing reports on the current state of information security programmes and governance issues in the organisation to the Board and the Senior Management; even though they hardly respond to the effects.

In the same vein, another CISO participant expressed 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 what we are actually expecting. Because of the limited channels, feedback has been grossly poor. We are not getting and receiving regular feedback on the effectiveness and performance of existing policies, standards and information security programmes.

Another CISO participant added that:

> 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. This is important for the dissemination of information security-related materials such as new or adjusted policies, standards, procedures, and new or emerging threats and vulnerabilities.

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. It is argued that when an incident occurs, it is important for the affected organisation to report to appropriate regulatory bodies as well as anti-fraud advisory groups. In all, 60 per cent of 5 CISOs mentioned that metrics are ineffective due to limited resources. Also, 80 per cent of the participants noted that disclosure is challenging; but it is mandatory. While 40 per cent of 5 CISOs agreed with disclosure, 60 per cent disagreed.

Discussion of Key Findings

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 policies and resources required to ensure the security of information assets of their organisations, most of the CISO participants argued that they were not getting adequate resources and capabilities from the Board and the Senior Management.

Existing studies indicated that effective information security management in every organisation commences with adequate and objective risk evaluation and management (Hong et al., 2003; Ab Rahman & Choo, 2015). Their studies indicated that it is critical to conduct risk management because without it the organisation may not know the right and appropriate strategies to create to ensure the protection of customer and other vital information. The analysis implies that the Board and the Senior Management are not adequately directing the CISO to conduct risk analysis and evaluation, which would inform the strategies, policies, and processes to be formulated and endorsed. The results from the evaluation of risk determine the kind of risk control measures and techniques that will be deployed (Ismail et al., 2014). Also, existing studies indicated that if there are effective and swift internal controls and provision for contingencies, information security incident response rates are likely to be improved.

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 information security risks (Akinrolabu et al., 2019; Hemanidhi & Chimmanee, 2017). Studies indicated that organisations should make efforts to reduce information security threats and risks to the lowest possible or acceptable levels (Inskeep, 2019; Ionescu et al., 2019). It is argued that risk management is expected to start from asset enumeration, where all the information assets that require protection are identified. These assets

can be found and identified through software, hardware and people (Ionescu et al., 2019). From the results, the importance of risk profiling is established, and this agrees with the existing studies, which showed that it helps to identify the extent and level of protection each information asset needs to ensure their optimum security (Hemanidhi & Chimmanee, 2017). As revealed in the analysis, proper identification of risks is necessary for preparing mitigation programmes. In other words, if the risks and threats are identified on time, the organisation through its CISO could quickly prepare either preventive or mitigating programmes to prevent or mitigate them. This agrees with the existing studies, which argued that identification of risks makes mitigating efforts effective (Tubío Figueira et al., 2019).

From the results, 60 per cent of 5 CISOs mentioned that metrics are ineffective due to limited resources. Also, 80 per cent of the participants noted that disclosure is challenging; but it is mandatory. While 40 per cent of 5 CISOs agreed with disclosure, 60 per cent disagreed. Some studies showed that disclosure of incidents is necessary for others to learn from the experience (Hemanidhi & Chimmanee, 2017; Tubío Figueira et al., 2019). 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. Studies indicated that getting feedback from external stakeholders on incident and threat management could be an effective strategy for preventing cyber incidents and threats (Wagner et al., 2019).

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, which they need to use to access money whenever they need it. 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 when saving money in financial institutions in Nigeria. Improved confidence in the finance sector may, therefore, increase the banked population from the current level.

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. Digital finance stimulates growth, which in turn leads to improved GDP in developing economies. 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, which may occur where unauthorized people have access to personal details of customers. The study may help prevent issues such as identity theft, fraud, disclosure of financial habits, spending, pension plans, which may expose customers to a myriad of dangers and risks. The study may also lead to a greater embrace of alternative means of accessing financial services because of the assurances of safety measures in place.

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, which would otherwise not be possible except where appropriate information security is in place. Flexible and more convenient finance access will lead to improved customer services. One of the financial institutions studied is a custodian of a national economic infrastructure, which can impact national security. The study may, therefore, help to preserve national heritage and prevent the harm that can impact on national pride where there is the implementation of strategies that prevent cyber exploitation.

Conclusion and Recommendations

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. They mentioned that lack of information security awareness could also lead to circumventing technology controls, for example, sharing of passwords or writing down passwords, which can lead to exploitation of information assets. Based on the results, the following recommendations are suggested:

i. 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 to accelerate the implementation of strategies and practices which make information safe. When institutions are crafting information security strategies, it is essential to consider regulations requiring compliance in the applicable country. Several financial services companies, especially the ones within the banking sector and those that have a relationship with foreign companies, are to comply with specific regulations and standards. Banks in Nigeria are required to comply with ISO 27001 and PCI-DSS standards. The financial companies that relate to European organisations are to comply with the GDPR. All institutions in Nigeria are also required, effective August 2019, to comply with the Nigeria data protection regulation. Their compliance with ISO 27001 is beneficial in this regard. Compliance with information security standards helps to protect against cyber exploitation because it requires specific actions that prevent cyber exploitation. The study established that such a decision will deliver specific information security protection across people, process, and technology areas.

ii. 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 also check for the effectiveness of deployed controls to prevent loss due to cyber exploitation. Monitoring efforts should include the setup of security operations centres. Security operations centres enable organisations to centralise monitoring and have a focused approach to detecting potential cyber exploitation and taking action promptly. It is not enough to deploy controls; it is necessary to monitor possible violations and use the outcomes to achieve better security. Monitoring helps organisations achieve the full benefits of information security beyond the use of policies.

iii. Tracking for the effectiveness of controls (policies, processes, and tools) deployed to prevent cyber exploitation is vital to stay secure. All of the participants mentioned that they do regular vulnerability assessments internally. They said that twice a year, they call in external vulnerability assessors to check weaknesses in their systems so they can fix them before any bad actors do. They all have internal control units that check that people are adhering to safe computing practices. They conduct clean desk sweeps to ensure confidentiality; they check that HR conducts processes such as background checks as and when due to prevent cyber

exploitation. They also check that staff do not misuse access rights on applications , and also that password policies on information systems are correctly set.

iv. 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. It appears that the practice of recording information security strategies explicitly across all lines of action is not common within financial services yet in Nigeria. Organisations only have risk management practices and supporting processes and policies, which include plans to prevent violations of information security. One critical step that is needed now is to document information security strategies as actionable plans across all elements for the future.

References

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

Abraham, S., & Chengalur-Smith, I. (2019). Evaluating the effectiveness of learner controlled information security training. *Computers & Security, 87,* 101586. doi: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'sa 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,* 101600. doi: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).

Ali, A., Warren, D., & Mathiassen, L. (2017). Cloud-based business services innovation: A risk management model. *International Journal of Information Management, 37*(6), 639-649. doi:10.1016/j.ijinfomgt.2017.05.008

Andress, J., & Leary, M. (2017). Develop an information security strategy. *Building A Practical Information Security Program*, 23-34. doi:10.1016/b978-0-12-802042-5.00002-0

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. Retrieved from https://www.cbn.gov.ng/out/2018/bsd/risk%20based%20cybersecurity%20framework%20exposure%20draft%20june.

Bauer, S., Bernroider, E., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security, 68*, 145-159. doi:10.1016/j.cose.2017.04.009

Central Bank of Nigeria. (2015). *Regulatory and supervisory guidelines for development finance institutions in Nigeria*. Retrieved from https://www.cbn.gov.ng/

Central Bank of Nigeria. (2018). *National Financial Inclusion Strategy(Revised).* Retrieved from https://www.cbn.gov.ng/

Central Bank of Nigeria. (2019). *Nigeria Financial Services Industry IT Standards Blueprint.* Retrieved from https://www.cbn.gov.ng/

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. doi:10.3233/KES-180384

de Gusmão, A., e Silva, L., Silva, M., Poleto, T., & Costa, A. (2016). Information security risk analysis model using fuzzy decision theory. *International Journal of Information Management, 36*(1), 25-34. doi:10.1016/j.ijinfomgt.2015.09.003

Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. *Computers & Security, 92,* 101747. doi:10.1016/j.cose.2020.101747

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.

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. doi: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. doi:10.1016/j.cose.2018.10.006

Hammer, M. J. (2016). Informed consent in the changing landscape of research. *Oncology Nursing Forum, 43*(5), 558-560. doi:10.1188/16.ONF.558-560

Han, Z., Huang, S., Li, H., & Ren, N. (2016). Risk assessment of digital library information security: a case study. *Electronic Library, 34*(3), 471-487. doi:10.1108/EL-09-2014-0158

Haqaf, H., & Koyuncu, M. (2018). Understanding key skills for information security managers. *International Journal of Information Management, 43,* 165-172. doi:10.1016/j.ijinfomgt.2018.07.013

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. Retrieved from http://jict.uum.edu.my/

Hinchliffe, A. (2017). Nigerian princes to kings of malware: the next evolution in Nigerian cybercrime. *Computer Fraud & Security*, 2017(5), 5-9. doi: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. doi:10.1108/09685220310500153

Hooper, V., & McKissack, J. (2016). The emerging role of the CISO. *Business Horizons, 59*(6), 585-591. doi:10.1016/j.bushor.2016.07.004

Ikusika, B. (2022). A critical analysis of cybersecurity in nigeria and the incidents of cyber-attacks on businesses/companies. *Companies (July 15, 2022)*.

Inskeep, T. (2019). How to properly position the CISO for success. *Security: Solutions for Enterprise Security Leaders, 56*(5), 36–37.

Ionescu, R. C., Grab, B., & Hassani, Y. (2019). Study of effects of information security management system in the context of the E.U. G*eneral Data Protection Regulation Application: Acces La Success. Calitatea, 20,* 322-328.

Ismail, S., Sitnikova, E., & Slay, J. (2014). Using integrated system theory approach to assess security for SCADA systems cybersecurity for critical infrastructures: A pilot study. 2014 11th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD). doi:10.1109/fskd.2014.6980976

Karanja, E. (2017). The role of the chief information security officer in the management of IT security. *Information & Computer Security, 25*(3), 300. doi:10.1108/ICS-02-2016-0013

Kern, F. (2016). The trials and tribulations of applied triangulation: Weighing different data sources. *Journal of Mixed Methods Research, 12*(2), 166-181. doi:10.1177/1558689816651032

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

Labrecque, L. I., Markos, E., Swani, K., & Peña, P. (2021). When data security goes wrong: Examining the impact of stress, social contract violation, and data type on consumer coping responses following a data breach. *Journal of Business Research*, *135*, 559-571.

Lanz, J. (2017). The chief information security officer: The new CFO of information security. CPA *Journal, 87*(6), 52-57. Retrieved from https://www.cpajournal.com/

Leung, D., Lo, A., Fong, L., & Law, R. (2015). Applying the Technology-Organization-Environment framework to explore ICT initial and continued adoption: An exploratory study of an independent hotel in Hong Kong. *Tourism Recreation Research, 40*(3), 391-406. doi:10.1080/02508281.2015.1090152

Madill, A., & Sullivan, P. (2018). Mirrors, portraits, and member checking: Managing difficult moments of knowledge exchange in the social sciences. *Qualitative Psychology, 5*(3), 321–339. doi:10.1037/qup0000089

Meriah, I., & Arfa Rabai, L. (2019). Comparative study of ontologies based ISO 27000 series security standards. *Procedia Computer Science, 160,* 85-92. doi:10.1016/j.procs.2019.09.447

National Information Technology Development Agency. (2019). Nigeria Data Protection Regulation. Retrieved from https://nitda.gov.ng/wp-content/uploads/2019/01/NigeriaDataProtectionRegulation.pdf

Ngwu, F. (2014). Promoting formal financial inclusion in Africa: An institutional re-examination of the policies with a case study of Nigeria. *Journal of Banking Regulation, 16*(4), 306-325. doi:10.1057/jbr.2014.13

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. doi:10.1057/s41303-016-0025-y.

Nish, A., Naumann, S., & Muir, J. (2022). *Enduring cyber threats and emerging challenges to the financial sector*. Carnegie Endowment for International Peace.

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*(02), 281-313. doi: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*.

Ozili, P. (2018). Impact of digital finance on financial inclusion and stability. *Borsa Istanbul Review, 18*(4), 329-340. doi:10.1016/j.bir.2017.12.003

Paananen, H., Lapke, M., & Siponen, M. (2020). State of the art in information security policy development. *Computers & Security, 88,* 101608. doi:10.1016/j.cose.2019.101608

Rae, K., Sands, J., & Subramaniam, N. (2017). Associations among the five components within COSO internal control-integrated framework as the underpinning of quality corporate governance. *Australasian Accounting Business & Finance Journal, 11*(1), 28–54. doi:10.14453/aabfj.v11i1.4

Rasekh, A., Hassanzadeh, A., Mulchandani, S., Modi, S., & Banks, M. (2016). Smart water networks and cybersecurity. *Journal of Water Resources Planning and Management, 142*(7), 01816004. doi:10.1061/(asce)wr.1943-5452.0000646.

Reece, R., & Stahl, B. (2015). The professionalization of information security: Perspectives of UK practitioners. *Computers & Security, 48,* 182-195. doi:10.1016/j.cose.2014.10.007

Ros, G. (2020). The making of a cyber crash: a conceptual model for systemic risk in the financial sector. *ESRB: Occasional Paper Series*, (2020/16).

Saunders, B., Kitzinger, J., & Kitzinger, C. (2015). Participant anonymity in the internet age: From theory to practice. *Qualitative Research in Psychology, 12(*2), 125-137. doi:10.1080/14780887.2014.948697

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. doi: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).

Thomaidis, A. (2022). Data breaches in hotel sector according to general data protection regulation (EU 2016/679). In *Tourism Risk: Crisis and Recovery Management* (pp. 129-140). Emerald Publishing Limited.

Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security awareness on information technology professionals' behavior. *Computers & Security, 79,* 68-79. doi:0.1016/j.cose.2018.08.007

Tubío Figueira, P., López Bravo, C., & Rivas López, J. (2019). Improving information security risk analysis by including threat-occurrence predictive models. *Computers & Security, 88,* 101609. doi:10.1016/j.cose.2019.101609

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, May). The vulnerability of the financial system to a systemic cyberattack. In *2021 13th International Conference on Cyber Conflict (CyCon)* (pp. 95-110). IEEE.

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

Wagner, T., Mahbub, K., Palomar, E., & Abdallah, A. (2019). Cyber threat intelligence sharing: Survey and research directions. *Computers & Security, 87,* 101589. doi:10.1016/j.cose.2019.101589

Yin, R. K. (2013). Validity and generalization in future case study evaluations. *Evaluation, 19*, 321–332. doi:10.1177/1356389013497081