ISSN: 2240 - 3855
Volume 10, Number 1, 2025
The Journal of Accounting and Management Research

CYBERSECURITY MEASURES AND THE INTEGRITY OF FINANCIAL REPORTING IN NIGERIA'S BANKING SECTOR.

Dr. Amadi-Robert, Wofuru[1] & Solomon Abuba[2]
[1]Department of Accountancy, Ignatius Ajuru University of Education,
[1]Mail:amwofuru@gmail.com, +234 806 314 0077
[2]solomon_abuba@hotmail.com

ABSTRACT
This study investigated the relationship between cybersecurity measures and the integrity of financial reporting in Nigeria's banking sector, with a specific focus on commercial banks in Rivers State. The integrity of financial reporting was defined in terms of accuracy, timeliness, and reliability, while cybersecurity measures included encryption, firewalls, multi-factor authentication, and employee training. A descriptive survey design was adopted, and data were obtained through structured questionnaires administered to 355 sampled employees across 24 commercial banks. Out of these, 340 questionnaires were duly completed and analyzed, representing a 96% response rate. Data were analyzed using descriptive statistics and Spearman Rank Correlation to test the study's hypotheses. The findings revealed that firewalls and encryption significantly enhanced reporting accuracy by preventing data manipulation and unauthorized access. Multi-factor authentication demonstrated a strong negative relationship with fraud, thereby improving financial transparency. Furthermore, cybersecurity training significantly improved the timeliness and reliability of financial reports by equipping employees with the skills to identify and mitigate risks. The results confirmed the relevance of the Technology Acceptance Model and the Resource-Based View, which emphasized cybersecurity tools as strategic resources for transparency. The study concluded that adopting robust cybersecurity measures was critical for safeguarding financial reporting integrity. It recommended sustained investment in encryption, mandatory multi-factor authentication, regular training, and stronger IT compliance frameworks.

Keywords: Cybersecurity, financial reporting integrity, firewalls, encryption, multi-factor authentication, Nigeria's banking sector

INTRODUCTION
The integrity of financial reporting has become a global concern, particularly in the banking sector where accuracy and reliability of financial statements are critical for investor confidence, regulatory oversight, and market stability. In Nigeria, the banking industry plays a pivotal role in economic growth by mobilizing savings, allocating credit, and facilitating financial intermediation. However, the rapid digitalization of banking operations has exposed financial reporting processes to increased cybersecurity threats, raising questions about data integrity, transparency, and accountability (Afolabi & Igbokwe, 2022). Cyberattacks such as hacking, phishing, and ransomware not only disrupt financial systems but also compromise sensitive financial data, leading to misstatements and loss of stakeholder trust (Okereke, 2020).

Globally, regulators and financial institutions have recognized cybersecurity as a key determinant of financial reporting integrity. In Nigeria, the Central Bank of Nigeria (CBN) and the Nigerian Deposit Insurance Corporation (NDIC) have mandated stricter IT governance and security frameworks to safeguard reporting systems (Ibrahim & Kasim, 2022). Despite these measures, persistent breaches and weak IT controls in some banks reveal gaps in implementation. Thus, strengthening cybersecurity is no longer an option but a necessity to ensure the integrity of financial reports.

Furthermore, the increasing sophistication of cybercrime in Nigeria has heightened the vulnerability of financial institutions, making it evident that traditional approaches to safeguarding data are insufficient. Banks are now confronted with dual challenges: adopting advanced cybersecurity frameworks and simultaneously building employee awareness to combat social engineering attacks. Failure to address these threats not only distorts the accuracy and timeliness of financial reports but

also exposes banks to reputational risks, litigation, and regulatory sanctions. This underscores the urgent need for empirical investigations into how cybersecurity measures influence the integrity of financial reporting in Nigeria's banking sector.

Statement of the Problem

Despite increased investment in IT infrastructure and the enforcement of regulatory guidelines, Nigerian banks still experience frequent cyberattacks that compromise the accuracy, reliability, and timeliness of financial reports. Cybersecurity breaches often result in data manipulation, fraudulent reporting, and delayed disclosures, all of which undermine the credibility of financial statements. This has severe implications for investor trust, corporate governance, and compliance with international financial reporting standards.

More critically, the absence of robust cybersecurity measures such as advanced encryption, firewalls, multi-factor authentication, and staff training exacerbates the situation, leaving financial data vulnerable to manipulation. While some banks have adopted partial security frameworks, the inconsistent implementation across the sector reflects gaps in commitment, expertise, and regulatory enforcement. As a result, financial reporting in Nigeria's banking industry continues to face questions about its integrity, threatening not only the stability of individual institutions but also the resilience of the entire financial system.

Objectives of the Study

The main objective of this study is to examine the relationship between cybersecurity measures and the integrity of financial reporting in Nigeria's banking sector. The specific objectives are to:

1. Determine the effect of firewalls and encryption on the accuracy of financial reporting.
2. Examine the relationship between multi-factor authentication and fraud prevention in financial reports.
3. Assess the impact of cybersecurity training on reporting timeliness and reliability.

Research Questions

1. To what extent do firewalls and encryption affect the accuracy of financial reporting?
2. How does multi-factor authentication contribute to fraud prevention in financial reports?
3. What role does cybersecurity training play in ensuring reporting timeliness and reliability?

Research Hypotheses

H_{01}: Firewalls and encryption have no significant effect on the accuracy of financial reporting.
H_{02}: Multi-factor authentication has no significant relationship with fraud prevention in financial reports.
H_{03}: Cybersecurity training has no significant impact on reporting timeliness and reliability.

Significance of the Study

This study will be valuable to:
Banks: by highlighting cybersecurity tools that improve reporting integrity.
Regulators: for designing effective IT compliance policies.
Investors: by reinforcing trust in financial disclosures.
Academics: as a reference for further research on cybersecurity and reporting.
Policy Makers: to strengthen national cybersecurity frameworks in the financial sector.

Scope of the Study

The study covers commercial banks in Nigeria, with emphasis on cybersecurity measures (firewalls, encryption, multi-factor authentication, and training) and financial reporting integrity (accuracy, timeliness, and reliability).

Definition of Terms

Cybersecurity Measures: Strategies and technologies designed to protect digital systems from cyber threats.

Financial Reporting Integrity: The accuracy, reliability, and timeliness of financial statements.

Encryption: Conversion of financial data into codes to prevent unauthorized access.

Multi-Factor Authentication: A security process requiring multiple forms of identification before granting system access.

LITERATURE REVIEW

Conceptual Review

Cybersecurity Measures

Cybersecurity measures encompass a wide range of technologies, policies, and practices designed to safeguard information systems against malicious threats, unauthorized access, and data breaches. In the banking sector, these measures have become indispensable because of the increasing reliance on digital platforms for financial transactions and reporting. According to Afolabi and Igbokwe (2022), cybersecurity tools such as firewalls, encryption, and intrusion detection systems serve as the first line of defense in preventing unauthorized manipulation of financial data. The adoption of multi-layered security protocols is essential for banks, given the sensitive nature of financial reporting, which requires both confidentiality and integrity. Without effective cybersecurity measures, financial reporting systems become highly vulnerable to inaccuracies, fraud, and reputational risks that can destabilize banking institutions.

Beyond technical defenses, cybersecurity measures also involve organizational policies and regulatory compliance. The Central Bank of Nigeria has issued several guidelines mandating banks to adopt cybersecurity frameworks that align with global standards such as ISO/IEC 27001. These frameworks are designed to create a structured environment where risks are continuously assessed, and preventive actions are taken to mitigate them (Ibrahim & Kasim, 2022). Umeh and Abang (2021) emphasize that banks that integrate cybersecurity into their corporate governance structures are better positioned to ensure the credibility of financial reports and enhance stakeholder trust. Thus, cybersecurity measures go beyond technologythey represent a culture of vigilance and accountability in the digital era.

Furthermore, the effectiveness of cybersecurity in safeguarding financial reporting depends on continuous adaptation to evolving threats. Cybercriminals employ increasingly sophisticated methods, including phishing, ransomware, and advanced persistent threats, which challenge traditional security systems (Okereke, 2020). As a result, banks must combine reactive measures with proactive strategies such as threat intelligence sharing, penetration testing, and regular updates to defense mechanisms. Recent studies highlight that institutions with stronger cybersecurity investments report fewer incidences of fraudulent reporting and data breaches, thereby improving transparency and regulatory compliance (Nwankwo & Okafor, 2021). This reinforces the role of cybersecurity as a cornerstone in maintaining financial reporting integrity in Nigeria's banking sector.

Financial Reporting Integrity

Financial reporting integrity refers to the degree to which financial statements are accurate, reliable, and free from manipulation or bias, ensuring that stakeholders can make informed decisions. According to Egbunike and Okoro (2018), integrity in reporting requires adherence to international accounting standards, ethical principles, and timely disclosures. In the banking sector, this concept is particularly significant because financial institutions handle public funds, and their reports influence both investor decisions and regulatory oversight. When reporting integrity is compromised, it leads to misinformation, weakens market confidence, and increases systemic risks in the financial sector.

The concept of financial reporting integrity also encompasses timeliness, which ensures that stakeholders receive relevant information when it is most useful for decision-making. Delays in

reporting can misrepresent the true financial position of banks, affecting the credibility of their operations (Oba, 2020). Integrity also requires consistency in applying accounting policies and transparency in disclosing risks and uncertainties. Studies show that firms with high levels of transparency enjoy lower costs of capital and higher investor trust, while those with opaque practices face reputational risks and reduced access to financing (Bushman & Smith, 2003). Thus, maintaining integrity in reporting is both a regulatory necessity and a strategic advantage in competitive financial markets.

In Nigeria, the challenge of ensuring reporting integrity is compounded by weak IT systems and frequent cybersecurity breaches. Fraudulent activities, insider manipulation, and cyberattacks have led to cases of misstated financial results, raising doubts about the reliability of reports from some banks (Okereke, 2020). According to Adekunle and Iyamu (2021), even when banks comply with International Financial Reporting Standards (IFRS), lapses in IT governance and cybersecurity controls often undermine reporting quality. Consequently, banks must integrate financial reporting integrity with robust cybersecurity systems to ensure that accuracy, timeliness, and reliability are not compromised. This underscores the interdependence between cybersecurity and reporting practices in modern banking.

Encryption & Firewalls

Encryption and firewalls represent two of the most critical cybersecurity measures for ensuring the accuracy and confidentiality of financial reporting. Encryption involves converting sensitive financial data into coded formats that can only be accessed with authorized decryption keys, thereby preventing data tampering during transmission or storage. Okereke (2020) notes that encryption has become a global standard for securing financial information, especially with the rise of online banking and electronic reporting. Firewalls, on the other hand, serve as barriers that filter traffic between trusted internal systems and untrusted external networks, blocking unauthorized access. Together, these tools ensure that financial data remains accurate and protected from cyber intrusions.

In the Nigerian banking sector, encryption and firewalls are critical in protecting financial reporting systems from common attacks such as hacking and malware. Uadiale and Oghoghomeh (2020) found that banks with stronger investments in encryption technologies reported fewer cases of financial misstatements caused by unauthorized system access. Similarly, studies suggest that firewalls not only reduce cyber threats but also ensure data consistency by monitoring suspicious traffic that could alter reporting records (Ibrahim & Kasim, 2022). However, while these technologies are effective, their success depends on continuous upgrades and alignment with evolving threats. Static or outdated encryption algorithms and firewall configurations expose financial data to breaches that undermine reporting integrity.

The adoption of encryption and firewalls also has broader implications for regulatory compliance and stakeholder trust. Regulators such as the CBN increasingly require banks to demonstrate evidence of secure IT environments as part of compliance with financial disclosure standards (Nwachukwu & Onyema, 2021). For investors and stakeholders, assurance that financial data is encrypted and protected enhances confidence in the reported figures. Nonetheless, high implementation costs and limited technical expertise remain barriers for many banks, particularly in developing economies like Nigeria (Obazee, 2021). Thus, while encryption and firewalls are vital for securing financial reporting systems, their effectiveness requires sustained investments, training, and regulatory enforcement to guarantee financial reporting integrity.

Theoretical Review

Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM), introduced by Davis (1989), has become one of the most influential frameworks for explaining technology adoption behavior. The model posits that two main factors perceived usefulness (PU) and perceived ease of use (PEOU)determine an individual's intention to adopt and effectively use technology. In the context of cybersecurity, perceived

usefulness relates to how much bank employees believe that encryption, firewalls, and multi-factor authentication will enhance the accuracy and security of financial reporting. Perceived ease of use, on the other hand, reflects the extent to which these tools are seen as user-friendly and requiring minimal effort. Empirical studies have validated TAM in banking, demonstrating that adoption of IT tools often depends on user perceptions rather than purely technical benefits (Sharma & Sharma, 2021). Thus, TAM provides a strong foundation for analyzing why banks adopt or resist cybersecurity tools for financial reporting.

Beyond individual acceptance, TAM has been applied in organizational settings to assess readiness for digital transformation. Kumar and Mishra (2020) observed that banks that provide adequate training and create awareness of cybersecurity benefits record higher adoption levels of security technologies. For instance, automation and encryption tools are more readily accepted when employees perceive them as reducing workloads and protecting them from liability for misreporting. Conversely, resistance to adopting complex security protocols often arises when employees view them as burdensome or time-consuming, even if they improve accuracy. In Nigeria, where IT literacy levels vary across banking staff, TAM highlights the importance of designing cybersecurity systems that are intuitive and supported by training to ensure widespread adoption.

Furthermore, TAM underscores the importance of external factors, such as management support and regulatory pressure, in shaping perceptions of usefulness and ease of use. Yakubu and Dasuki (2019) argued that in developing economies, employees' willingness to adopt IT systems increases when management integrates cybersecurity into performance evaluations and when regulators emphasize compliance. In this light, TAM does not only predict individual attitudes but also explains organizational dynamics in adopting cybersecurity for financial reporting. In Nigeria's banking sector, where frequent cyber breaches have raised doubts about reporting integrity, TAM remains relevant in analyzing how perceptions influence the adoption and sustained use of cybersecurity measures.

Resource-Based View (RBV)

The Resource-Based View (RBV), popularized by Barney (1991), argues that organizations achieve sustainable competitive advantage by acquiring and deploying resources that are valuable, rare, inimitable, and non-substitutable (VRIN). Within the banking sector, cybersecurity systems such as advanced encryption, robust firewalls, and specialized IT expertise represent strategic resources that can enhance the accuracy, timeliness, and reliability of financial reporting. By safeguarding financial data from manipulation, these resources directly contribute to reporting integrity and stakeholder confidence. Adeniyi and Ayodele (2020) emphasized that banks that strategically invest in unique cybersecurity frameworks enjoy a competitive edge because stakeholders perceive their reports as more reliable. This makes cybersecurity not just a technical necessity but also a strategic resource that strengthens organizational legitimacy.

RBV also highlights the role of intangible resources such as human expertise and organizational culture in sustaining competitive advantage. Ogbonna and Chukwu (2021) found that while cybersecurity technologies are crucial, their effectiveness depends on employees' technical skills and awareness. A highly trained IT workforce that can anticipate and mitigate emerging threats becomes an inimitable resource, as competitors cannot easily replicate tacit knowledge and organizational culture. In the Nigerian banking sector, where skilled cybersecurity experts are scarce, human capital development becomes as vital as technological investment. This aligns with RBV's argument that a combination of tangible and intangible resources sustains superior performance over time.

In addition, RBV suggests that firms that fail to develop robust cybersecurity capabilities risk losing competitive advantage and stakeholder trust. Okoye and Mba (2019) noted that banks with weak IT infrastructures and poor security measures experienced more frequent financial misreporting, damaging their reputations and increasing regulatory scrutiny. In contrast, banks that integrated cybersecurity into their strategic planning not only improved transparency but also attracted more investors due to increased confidence in their disclosures. Thus, RBV reinforces the notion that cybersecurity frameworks are not just defensive tools but strategic resources that can differentiate high-performing banks from laggards in Nigeria's financial sector.

2.2.3 Stakeholder Theory

Stakeholder Theory, advanced by Freeman (1984), argues that organizations exist within a network of relationships involving multiple stakeholderssuch as shareholders, regulators, customers, employees, and societyand must balance their interests to maintain legitimacy. In the context of financial reporting, this theory emphasizes that banks must ensure transparency and data integrity to fulfill their obligations to these stakeholders. Eke and Chikezie (2021) noted that when banks adopt cybersecurity measures to protect financial reports from manipulation, they demonstrate accountability not just to regulators but also to customers and investors who rely on accurate information for decision-making. Thus, the integrity of financial reporting becomes a way of fulfilling ethical and legal obligations to stakeholders.

The adoption of cybersecurity measures directly aligns with stakeholder expectations of trust, security, and accountability. Babalola and Ogunleye (2021) observed that cyber breaches in financial institutions often result in significant reputational damage because they are viewed as failures to safeguard stakeholder interests. In Nigeria, where public confidence in the banking sector is already fragile due to past financial scandals, cybersecurity lapses can amplify distrust. By embedding robust security frameworks, banks signal their commitment to protecting stakeholder interests, which enhances legitimacy and ensures compliance with governance standards. This reinforces the central proposition of Stakeholder Theorythat legitimacy and long-term success are tied to meeting stakeholder expectations.

Furthermore, Stakeholder Theory has implications for regulatory frameworks and corporate governance. Okon and Idoko (2021) argued that regulators, as key stakeholders, demand higher levels of cybersecurity compliance from banks to prevent systemic risks in the financial system. Banks that neglect these expectations risk penalties, litigation, and reputational losses that could undermine their survival. On the other hand, banks that consistently meet or exceed stakeholder expectations through transparent reporting and secure IT systems are more likely to gain long-term sustainability. In this regard, Stakeholder Theory not only explains the ethical rationale for adopting cybersecurity measures but also provides a practical justification for why Nigerian banks must invest in protecting the integrity of financial reporting.

Empirical Review

Ogbonna and Ebuehi (2019) investigated the effect of accounting systems automation on the timeliness of financial reporting in Nigerian commercial banks. Using a survey design, the authors sampled 250 bank staff across Lagos and Abuja, combining structured questionnaires with follow-up interviews for triangulation. Their quantitative analysis (Pearson correlation and regression) showed that automation of routine accounting tasks including automated journal entries, reconciliation routines and report generation significantly reduced the time taken to produce statutory and management reports. Respondents reported fewer manual adjustments, shorter close cycles, and improved ability to meet regulatory deadlines. The study also flagged implementation barriers (user resistance, inadequate training, and legacy system incompatibilities) that moderated the automation benefit. Methodologically the study was robust in design but limited by its geographic focus (Lagos/Abuja) and reliance on self-reported measures of timeliness. For your study, Ogbonna and Ebuehi's findings are important because they demonstrate how automation (often secured and enabled by cybersecurity systems) reduces reporting delays; this supports the idea that cybersecurity investments that protect automated workflows indirectly improve the timeliness dimension of reporting integrity

Afolabi and Igbokwe (2022) examined the relationship between specific cybersecurity measures (encryption, firewalls, and multi-factor authentication) and the accuracy of financial statements in Nigerian deposit money banks. The researchers adopted a cross-sectional survey of 250 accountants and IT personnel across a purposive sample of banks, supplemented with a review of reported security incidents over a five-year period. Using logistic regression, they found that banks with formal encryption policies, up-to-date cryptographic implementations, and enforced multi-factor authentication recorded significantly fewer incidents of data tampering and misstatements.

Importantly, the study linked technical controls to observable improvements in audit trails and reconciliations, which auditors used to corroborate account balances. Limitations included potential survivorship bias (banks that suffered large breaches were sometimes underrepresented) and limited access to internal breach logs. For your study, Afolabi and Igbokwe provide direct empirical evidence that technical cybersecurity measures strengthen the accuracy pillar of financial reporting integrity an essential foundation for arguing that encryption and authentication should be prioritized in Nigerian banks

Umeh and Abang (2021) analyzed how weak cybersecurity posture contributed to incidents of financial misreporting in Nigerian financial institutions. Employing a mixed-methods approach, they combined an industry survey of 180 finance and IT professionals with eight case studies of documented cyber incidents in banks and microfinance institutions. Their qualitative analysis revealed common causal chains: phishing/social engineering led to credential compromise unauthorized transactions or data alterations delayed or manipulated reporting to conceal the breach. Quantitatively, organizations reporting low maturity on cybersecurity frameworks scored higher on reported instances of post-close adjustments and restatements. The study concluded that inadequate cyber hygiene, poor employee awareness, and weak incident response amplified the risk that cyber events would translate into compromised financial reports. Umeh and Abang's work is particularly relevant to your study because it establishes the mechanisms by which cybersecurity weaknesses become reporting-integrity problems, supporting the need to examine both technical controls and human factors

Ibrahim and Kasim (2022) evaluated the role of IT governance frameworks (policy, risk management, incident response, and third-party controls) in protecting financial reporting integrity across Nigerian banks. Using a survey of 160 compliance officers and C-level IT managers plus documentary analysis of bank governance reports, they applied factor analysis to derive governance maturity dimensions and then correlated maturity scores with measures of reporting reliability (frequency of restatements, auditor qualifications, and timeliness). The study found a strong, positive association between governance maturity and reporting integrity: banks with formal IT risk registers, tested incident response plans, and rigorous vendor controls were less likely to experience data loss or misstatements. However, the research noted under-utilization of these frameworks: many banks had policies on paper but weak operationalization. For your research, Ibrahim and Kasim underscore the institutional side of cybersecurity that technology alone is insufficient unless governance translates policy into practice, reinforcing the study's interest in both controls and organizational readiness

Okereke (2020) conducted an empirical investigation into cyber threats (ransomware, malware, and targeted attacks) and their immediate impact on financial data integrity within selected Nigerian banks. The author used archival incident records from regulatory filings and internal audit reports spanning 2016–2019 and applied descriptive and event-study methods to assess short-term effects on reported financials. Okereke found that major cyber incidents were often followed by late disclosures, material adjustments in subsequent financials, and increased auditor scrutiny. The study emphasized technical deficiencies (outdated patching, weak encryption standards) as root causes that allowed attackers to alter or exfiltrate data. Limitations included uneven availability of incident details and potential underreporting. For your article, Okereke offers historical, incident-based evidence linking cyberattacks to measurable deterioration in reporting integrity, which strengthens the causal argument that better cybersecurity reduces misreporting risks

Obazee (2021) explored barriers to effective IT and cybersecurity adoption among Nigerian small and medium financial institutions (including smaller banks). Through survey research and semi-structured interviews with 180 managers and IT staff, Obazee identified lack of specialized skills, limited budgets, and poor vendor governance as recurring obstacles. The study's statistical analysis showed that these constraints not only limited system deployment but also reduced the operational effectiveness of security controls (e.g., improper configurations, expired certificates). The practical consequence was that many controls existed in name only and failed under targeted attacks, with subsequent implications for data accuracy and auditability. Though focused on smaller institutions,

Obazee's conclusions are relevant to larger banks in regions with constrained infrastructure (like some branches in Rivers State): even where technical solutions are theoretically available, human and resource constraints can blunt their effect on reporting integrity

Nwankwo and Okafor (2021) examined the moderating role of regulatory enforcement on the effectiveness of cybersecurity investments in enhancing financial reporting transparency. Using qualitative content analysis of CBN circulars, NDIC guidance, and interviews with 120 senior banking professionals, they argued that strong regulatory enforcement (timely audits, penalties for non-compliance, and mandatory disclosure rules) amplified the positive effects of cybersecurity measures. Banks operating under active regulatory scrutiny were more likely to convert cybersecurity spending into operational controls and audit evidence resulting in fewer restatements and greater investor confidence. The study cautioned, however, that inconsistent enforcement across regions undermined systemic resilience. For your research, their findings suggest exploring not only technical and organizational controls but also how external regulators and enforcement regimes enable or constrain the link between cybersecurity and reporting integrity

METHODOLOGY

Research Design

This study adopted a descriptive survey research design to investigate the relationship between cybersecurity measures and the integrity of financial reporting in Nigeria's banking sector. A descriptive survey is appropriate because it enables the researcher to collect data directly from respondents about their experiences, perceptions, and practices regarding cybersecurity and reporting. According to Creswell and Creswell (2018), survey designs are particularly suitable for studies that aim to establish associations between variables in real-world contexts, especially when experimental control is not possible. The design provides flexibility in gathering data from a large population across multiple banks, thereby improving the generalizability of the findings.

Furthermore, the descriptive survey design allows for the measurement of variables such as encryption, firewalls, multi-factor authentication, and cybersecurity training (independent variables) in relation to reporting accuracy, timeliness, and reliability (dependent variables). The design also supports the use of both descriptive statistics and inferential tests such as correlation, which are appropriate for identifying relationships between variables without manipulating them (Pallant, 2020). In the context of banking research, where operational environments cannot be experimentally altered, a descriptive survey offers the most practical and reliable method for achieving the research objectives.

Population of the Study

The population of this study comprised 3,200 employees drawn from 24 commercial banks operating in Rivers State, Nigeria, cutting across finance, IT, audit, risk management, and operations departments. This population was chosen because employees in these categories are directly involved in financial reporting processes and the use of cybersecurity tools. A broad population ensures that the perspectives captured reflect diverse departmental experiences in managing financial reporting risks.

Sample Size and Sampling Technqiues

The sample size was determined using Taro Yamane's (1967) formula at a 5% margin of error, which produced a sample of 355 respondents. Proportionate stratified random sampling was employed to ensure fair representation across banks and departments. This approach reduces bias by ensuring that larger banks with more employees contribute more respondents while smaller banks are still represented. Stratification by department also ensures that views from IT experts, finance officers, and auditors are included. According to Saunders et al. (2019), stratified sampling enhances representativeness and increases the reliability of conclusions. Thus, the final sample of 355 respondents is considered sufficient and statistically reliable for generalizing the study findings.

Sources of Data

The study relied primarily on primary data obtained directly from respondents through structured questionnaires. Primary data were chosen because they provide firsthand insights into employees' perceptions, practices, and experiences with cybersecurity and financial reporting integrity. Unlike secondary data, which may be outdated or aggregated, primary data allow for specific measurements aligned with the research objectives (Kothari, 2014).

Additionally, primary data collection ensured that variables such as multi-factor authentication, encryption, and staff training could be directly linked to outcomes such as reporting timeliness and accuracy. Secondary sources, including Central Bank of Nigeria guidelines, NDIC regulations, and prior academic studies, were used to support the conceptual framework but were not the main source of empirical evidence. Collecting firsthand data enhanced the validity of the research and allowed for contextual analysis relevant to Nigeria's banking environment.

Instrument of Data Collection

The main instrument for data collection was a structured questionnaire, which was designed in alignment with the study's objectives and hypotheses. The questionnaire consisted of two sections: Section A collected demographic data (gender, age, educational background, years of experience, and department), while Section B focused on the study variables. Items on cybersecurity measures included questions on the use of firewalls, encryption, multi-factor authentication, and cybersecurity training. Items on reporting integrity covered accuracy, timeliness, and reliability of financial statements.

A five-point Likert scale ranging from "Strongly Disagree (1)" to "Strongly Agree (5)" was employed to measure respondents' opinions and perceptions. This scaling technique is widely used in survey research as it captures the intensity of respondents' attitudes and perceptions while allowing for statistical analysis (Bryman, 2016). To ensure validity, the questionnaire was subjected to expert review by academics in accounting and information systems as well as IT managers from selected banks. A pilot test involving 30 respondents was also conducted to assess clarity, reliability, and consistency of the items, after which minor adjustments were made. The instrument's reliability was confirmed using Cronbach's alpha, which produced coefficients above the recommended threshold of 0.70, indicating internal consistency (Nunnally & Bernstein, 1994).

Data Analysis

Data collected were coded and entered into the Statistical Package for Social Sciences (SPSS) version 25 for analysis. Descriptive statistics such as means, standard deviations, frequencies, and percentages were used to summarize demographic information and highlight trends in responses. Descriptive analysis provided an overview of the prevalence of cybersecurity practices and the general state of financial reporting integrity among the surveyed banks.

For hypothesis testing, the Spearman Rank Correlation Coefficient was employed to examine the relationships between cybersecurity measures (independent variables) and financial reporting integrity (dependent variable). Spearman correlation was selected because the study variables were measured on ordinal scales (Likert-type items) and the test is robust for non-parametric data (Pallant, 2020). A 95% confidence interval was applied, with significance tested at $p < 0.05$. Results were presented in tables and interpreted in line with the study objectives.

The analysis method was chosen because it not only identifies the strength and direction of relationships but also provides a basis for drawing conclusions about the effect of cybersecurity on financial reporting integrity in the Nigerian banking sector. This aligns with the study's overall objective of empirically determining whether cybersecurity tools significantly influence the accuracy, reliability, and timeliness of financial reporting.

DATA PRESENTATION, ANALYSIS AND DISCUSSION

Data Presentation

Out of the 355 questionnaires distributed, 340 were properly completed and returned, giving a response rate of 96%, which is considered adequate for robust analysis. The high response rate enhances the reliability of the findings by minimizing non-response bias.

Table 4.1: Questionnaire Distribution and Response Rate

Distributed	Returned	Not Returned	Response Rate (%)
355	340	15	96%

Table 4.1 shows that the study achieved a very high response rate (96%), indicating strong cooperation from respondents. Such a response rate improves representativeness, ensuring that the results can be generalized to employees of commercial banks in Rivers State.

Table 4.2: Demographic Characteristics of Respondents

Variable	Category	Frequency	Percentage (%)
Gender	Male	198	58.2
	Female	142	41.8
Age	20–29 years	95	27.9
	30–39 years	145	42.6
	40–49 years	70	20.6
	50 years and above	30	8.9
Department	Finance/Accounts	110	32.4
	Audit/Control	60	17.6
	IT/Operations	120	35.3
	Risk/Compliance	50	14.7

Table 4.2 indicates that 58.2% of the respondents were male, while 41.8% were female, showing a balanced gender distribution. The majority (42.6%) of respondents were aged between 30 and 39 years, reflecting a workforce dominated by young professionals. Departmental distribution shows strong representation from IT/Operations (35.3%) and Finance/Accounts (32.4%), which is appropriate since these departments are most directly engaged in cybersecurity and financial reporting activities.

Hypotheses Testing

The study tested three hypotheses using Spearman Rank Correlation to assess the strength and direction of the relationship between cybersecurity measures and financial reporting integrity.

Hypothesis One

H_{01}: Firewalls and encryption have no significant effect on the accuracy of financial reporting.

Table 4.3: Correlation between Firewalls & Encryption and Reporting Accuracy

Variables	ρ (Spearman Correlation)	Sig. (p-value)	Decision
Firewalls & Encryption vs Reporting Accuracy	0.72	0.000	Reject H01

Table 4.3 shows a strong positive correlation ($\rho = 0.72$, $p < 0.05$) between firewalls/encryption and reporting accuracy. This implies that banks with strong encryption and firewall systems report significantly more accurate financial statements. Since $p < 0.05$, the null hypothesis (H01) is rejected, confirming that firewalls and encryption positively influence reporting accuracy.

Hypothesis Two

H_{02}: Multi-factor authentication has no significant relationship with fraud prevention in financial reports.

Table 4.4: Correlation between Multi-Factor Authentication and Fraud Prevention

Variables	ρ (Spearman Correlation)	Sig. (p-value)	Decision
Multi-Factor Authentication vs Fraud Prevention	0.81	0.000	Reject H02

Table 4.4 indicates a very strong positive correlation ($\rho = 0.81$, $p < 0.05$) between multi-factor authentication and fraud prevention. This means that banks employing multi-factor authentication experience fewer cases of fraud-related misreporting. The null hypothesis (H02) is rejected, showing that multi-factor authentication plays a critical role in strengthening fraud prevention and sustaining financial reporting integrity.

Hypothesis Three

H_{03}: Cybersecurity training has no significant impact on reporting timeliness and reliability.

Table 4.5: Correlation between Cybersecurity Training and Reporting Timeliness/Reliability

Variables	ρ (Spearman Correlation)	Sig. (p-value)	Decision
Cybersecurity Training vs Reporting Timeliness & Reliability	0.65	0.000	Reject H03

Table 4.5 reveals a moderately strong positive correlation ($\rho = 0.65$, $p < 0.05$) between cybersecurity training and reporting timeliness/reliability. This indicates that regular training of staff enhances their ability to prevent cyber risks, thereby improving the timeliness and dependability of reports. Since the p-value is below 0.05, the null hypothesis (H03) is rejected.

Discussion of Findings

The findings of this study revealed that cybersecurity measures play a significant role in enhancing the integrity of financial reporting in Nigeria's banking sector. Specifically, firewalls and encryption were strongly correlated with reporting accuracy, multi-factor authentication was positively associated with fraud prevention, and cybersecurity training contributed to timeliness and reliability of financial disclosures. Collectively, these results align with the propositions of the Technology Acceptance Model (TAM), the Resource-Based View (RBV), and Stakeholder Theory, which together provide a robust theoretical foundation for understanding the critical role of cybersecurity in safeguarding financial reporting.

First, the result showing a strong positive relationship between firewalls, encryption, and reporting accuracy supports the Technology Acceptance Model (Davis, 1989), which emphasizes that technologies are more readily adopted when perceived as useful and effective. In this case, employees recognized that encryption and firewalls ensured data accuracy and protected financial information from unauthorized access. This finding corroborates Afolabi and Igbokwe (2022), who

reported that encryption and authentication significantly improved financial reporting accuracy in Nigerian banks. Similarly, Okereke (2020) documented that weak encryption protocols often led to breaches and subsequent financial misreporting. The evidence confirms that firewalls and encryption are essential cybersecurity tools for enhancing the accuracy component of reporting integrity in Nigerian banks.

Second, the study found a very strong correlation between multi-factor authentication and fraud prevention. This outcome resonates with the RBV framework (Barney, 1991), which views unique security systems such as multi-factor authentication as valuable and inimitable resources that safeguard data integrity. By requiring multiple layers of identification, multi-factor authentication reduced opportunities for fraudulent manipulation of financial reports. This finding aligns with Umeh and Abang (2021), who argued that weak authentication systems were a major cause of financial misreporting in Nigerian institutions. Moreover, it confirms earlier evidence by Ibrahim and Kasim (2022), who noted that banks with stronger IT governance and authentication protocols experienced fewer fraud-related restatements. Thus, the result underscores that multi-factor authentication not only deters fraud but also strengthens the overall transparency of reporting.

Third, the significant relationship between cybersecurity training and reporting timeliness/reliability highlights the importance of human capital in sustaining IT investments. While technology provides the tools, its effectiveness depends on users' knowledge and vigilance. The finding supports Stakeholder Theory (Freeman, 1984), which emphasizes that organizations must safeguard stakeholder interests through secure and reliable financial information. Ibrahim and Kasim (2022) similarly stressed that staff training is essential for effective IT governance in Nigerian banks, while Obazee (2021) identified inadequate training as a key obstacle to achieving reporting transparency. In this study, regular cybersecurity training enhanced employees' ability to detect, prevent, and respond to cyber threats, thereby ensuring reports were both timely and reliable.

Overall, the results confirm that cybersecurity measures are indispensable for protecting financial reporting integrity in Nigeria's banking sector. However, the study also highlights persistent challenges such as weak IT infrastructure, uneven regulatory enforcement, and low cybersecurity literacy among employees. These findings echo Umeh and Abang (2021), who argued that inadequate infrastructure and skills often limit the effectiveness of cybersecurity adoption. Thus, while the adoption of cybersecurity tools strengthens accuracy, timeliness, and reliability of reporting, sustained investments in infrastructure, staff capacity building, and regulatory enforcement remain critical for achieving optimal outcomes.

SUMMARY, CONCLUSION AND RECOMMENDATIONS

Summary of Findings

This study examined the relationship between cybersecurity measures and the integrity of financial reporting in Nigeria's banking sector. Primary data were obtained from 340 respondents across 24 commercial banks in Rivers State, and the hypotheses were tested using Spearman Rank Correlation. The findings can be summarized as follows:

1. Firewalls and encryption significantly enhanced reporting accuracy. Banks with robust encryption protocols and firewall defenses produced more accurate financial statements by preventing unauthorized access and data tampering.
2. Multi-factor authentication reduced fraud risks in financial reporting. By requiring multiple verification processes, banks limited fraudulent activities and strengthened audit trails, thereby improving transparency.
3. Cybersecurity training improved timeliness and reliability of reports. Employees with adequate training were better able to detect, prevent, and respond to threats, which ensured timely and dependable disclosures.

These findings confirm that cybersecurity measures are critical in improving financial reporting integrity, consistent with earlier studies (Afolabi & Igbokwe, 2022; Umeh & Abang, 2021).

Conclusion

The study concludes that cybersecurity measures significantly contribute to the accuracy, timeliness, and reliability of financial reporting in Nigeria's banking sector. Banks that adopt advanced security tools such as encryption, firewalls, and multi-factor authentication are more likely to generate financial statements that inspire stakeholder confidence and meet regulatory expectations. Furthermore, investment in human capital through continuous cybersecurity training ensures that employees are equipped to apply these tools effectively, thereby strengthening the credibility of financial reports.

The results align with the Technology Acceptance Model (Davis, 1989) by showing that adoption of useful and user-friendly cybersecurity technologies promotes better reporting practices. They also support the Resource-Based View (Barney, 1991) by positioning cybersecurity frameworks as strategic resources that sustain competitive advantage through transparency. Finally, they reinforce Stakeholder Theory (Freeman, 1984) by highlighting that protecting financial information is central to fulfilling stakeholder expectations and maintaining legitimacy.

However, the study also recognizes persistent challenges such as weak IT infrastructure, inconsistent regulatory enforcement, and limited cybersecurity expertise. These constraints reduce the full realization of cybersecurity benefits in Nigerian banks. Therefore, sustained investment, policy support, and continuous employee capacity building are essential for safeguarding financial reporting integrity.

Recommendations

Based on the findings, the following recommendations are proposed:

1. Strengthen Encryption and Firewalls: Banks should expand investment in encryption technologies and firewalls to ensure data accuracy and protect financial reports from unauthorized manipulation.
2. Mandate Multi-Factor Authentication: Multi-factor authentication should be made compulsory for all financial data access points to minimize fraud risks and improve transparency.
3. Institutionalize Regular Cybersecurity Training: Banks should implement mandatory cybersecurity training programs to enhance employee awareness and improve reporting timeliness and reliability.
4. Develop Stronger IT Compliance Frameworks: Regulators such as the Central Bank of Nigeria (CBN) and the Nigerian Deposit Insurance Corporation (NDIC) should design and enforce robust IT governance policies to standardize cybersecurity practices across banks.
5. Integrate Cybersecurity into Corporate Governance: Banks should embed cybersecurity policies into their governance structures, linking reporting integrity to board oversight and internal control systems.

REFERENCES

Adekunle, O., & Iyamu, E. (2021). International Financial Reporting Standards (IFRS) compliance and reporting quality of Nigerian banks: The role of IT governance. *Journal of Accounting and Financial Management*, 12(3), 77–91.

Adeniyi, A., & Ayodele, O. (2020). Cybersecurity frameworks and competitive advantage in Nigerian banks: A resource-based perspective. *International Journal of Information Systems and Management*, 6(2), 101–117.

Afolabi, A., & Igbokwe, C. (2022). Cybersecurity measures and financial reporting accuracy in Nigerian deposit money banks. *Journal of Accounting and Financial Reporting*, 8(2), 45–62.

Babalola, O., & Ogunleye, S. (2021). Cybersecurity breaches and stakeholder trust in Nigerian deposit money banks. *Journal of Banking and Finance Management*, 9(3), 55–69.

Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, 17(1), 99–120.

Bushman, R. M., & Smith, A. J. (2003). Transparency, financial accounting information, and corporate governance. *Economic Policy Review*, 9(1), 65–87.

Davis, F. D. (1989). *Perceived usefulness, perceived ease of use, and user acceptance of information technology*. MIS Quarterly, 13(3), 319–340.

Egbunike, F. C., & Okoro, G. E. (2018). Financial reporting quality and corporate performance of quoted firms in Nigeria. *International Journal of Business and Management Review*, 6(3), 1–13.

Eke, G., & Chikezie, S. (2021). Stakeholder accountability and cybersecurity adoption in Nigerian financial institutions. A*frican Journal of Accounting, Auditing and Finance*, 7(2), 221–238.

Freeman, R. E. (1984). *Strategic management:* A stakeholder approach. Boston, MA: Pitman.

Ibrahim, M., & Kasim, R. (2022). IT governance frameworks and financial reporting integrity in Nigerian banks. *Journal of African Business*, 23(4), 567–584.

Kumar, R., & Mishra, S. (2020). Technology adoption in banking: Evidence from cybersecurity practices. J*ournal of Financial Innovation*, 5(1), 44–62.

Nwachukwu, A., & Onyema, E. (2021). Regulatory compliance and IT security in Nigerian financial institutions: Implications for reporting transparency. *African Journal of Accounting, Auditing and Finance*, 7(4), 321–339.

Nwankwo, O., & Okafor, C. (2021). Cybersecurity investment and financial reporting transparency in Nigerian banks. *Journal of Financial Reporting and Accounting*, 19(2), 205–222.

Oba, V. C. (2020). Corporate governance mechanisms and financial reporting timeliness in Nigeria. *International Journal of Accounting and Finance*, 9(1), 12–29.

Obazee, A. (2021). Barriers to IT adoption and cybersecurity effectiveness in Nigerian financial institutions. *International Journal of Accounting and Information Systems*, 22(2), 55–71.

Ogbonna, B. C., & Ebuehi, S. O. (2019). Accounting systems automation and timeliness of financial reporting in Nigerian commercial banks. *International Journal of Accounting and Management*, 7(1), 89–104.

Ogbonna, B., & Chukwu, E. (2021). Human capital and cybersecurity effectiveness in Nigerian banks: A resource-based view. *International Journal of Finance and Accounting*, 10(2), 71–85.

Okereke, J. O. (2020). Cyber threats and the integrity of financial data in Nigerian banks: Evidence from incident reports. *Journal of Financial Crime Studies*, 12(1), 77–92.

Okon, E., & Idoko, C. (2021). Regulatory enforcement, corporate governance, and cybersecurity in Nigerian banks: A stakeholder approach. *Journal of Corporate Governance Research*, 14(4), 150–167.

Okoye, A., & Mba, F. (2019). IT infrastructure and financial misreporting: Evidence from Nigerian deposit money banks. *Journal of Accounting and Information Systems,* 15(3), 245–259.

Sharma, R., & Sharma, S. (2021). Understanding user acceptance of cybersecurity tools in banking: Extending the Technology Acceptance Model. *Journal of Information Security Research*, 11(2), 89–104.

Uadiale, O. M., & Oghoghomeh, T. (2020). IT infrastructure and the quality of financial reporting in Nigerian service firms. *Journal of Accounting Research and Practice*, 14(2), 88–104.

Umeh, A., & Abang, D. (2021). Cybersecurity and corporate governance: Evidence from Nigerian deposit money banks. *International Journal of Corporate Governance*, 10(1), 44–59.

Yakubu, M., & Dasuki, S. (2019). Adoption of information systems in developing countries: A technology acceptance model approach. *African Journal of Information Systems*, 11(2), 69–86.