CYBER SECURITY RISK DISCLOSURE QUALITY AND ITS EFFECT ON INVESTOR CONFIDENCE IN NIGERIA'S FINANCIAL INSTITUTION

Onwe Nkiruka Ogayi, Onuoha Perpetua Ijeoma, Asu Fidelis Ndubuisi, Stephen Nwidembia Ikechukwu, Alo Sooky Nnenna, Nweze Ndidiamaka Benedicta, Ojimba Chidi Malachy
08065649575
onwenkirukavictoria@gmail.com

[1] *Accountancy Department, Faculty of Management Sciences*

Ebonyi State University Abakaliki, Nigeria

[2]*Accountancy Department , Faculty of Management Sciences*

[2]*Alex - Ekwueme Federal University Ndufu -Alike, Nigeria.*

Abstract

The paper focuses on investigating the practice of cybersecurity risk disclosure by financial institutions in Nigeria and the effect on investor confidence. The study also assesses the extent and standard of the disclosure, the elements affecting it, and the relationship between standard and confidence. As the study adopted a qualitative approach, it relied on secondary sources of data such as annual reports, ESG disclosures, regulatory documents, and literature. The thematic analysis conducted on governance matters, reporting of incidents, investment in infrastructure, awareness among customers, and transparency helped to assess the inter-linkages between disclosure and confidence of investors. The result shows a higher percentage (62%) of cybersecurity risk disclosure by multinational banks compared to indigenous banks (37%), which is largely due to the influence of global governance systems. The importance of cybersecurity risk disclosure is viewed by stakeholders, with priority considerations on governance (71%), reporting (65%), infrastructure (54%), and awareness (48%). Other important considerations are high implementation costs (67%), a shortage of qualified personnel (58%), inadequate regulatory support (53%), and low awareness (45%). Perceived assessments by the stakeholders indicate increased perceptions on trust (39%), risk management (37%), and investment (40%) due to high-quality cybersecurity risk disclosure. High-quality disclosure has a positive influence on 57% of stakeholders, and low-quality disclosure has a negative influence on 50%. Transparent and effective cybersecurity risk disclosure is very important to improve investor trust, operational resilience, investment decisions, and stability within the digital financial ecosystem of Nigeria.

Keywords: *Cybersecurity, Risk Disclosure, Investor Confidence, Nigerian Banks, Digital Banking, Financial Institutions*

INTRODUCTION

The Nigerian banking industry has, undergone a great transformation over the last two decades, which has been a result of digitalization, and today, internet banking, mobile banking, ATMs, POS, and other electronic banking platforms are at the heart of service delivery. Nevertheless, with the increased use of digital banking platforms, the risk of cyber-criminal activities such as cyber fraud, hacking, and other cybersecurity threats has also increased (Egenti, 2025; Garba et al., 2023).

Empirical research has indicated that Nigerian banks are not exempted from cybersecurity threats. An example is a study intended to evaluate the Internet banking security provided by Nigerian banks, where it indicated that, out of 100 surveyed banking and security professionals, 80 percent of the participants indicated exposure to at least one cybersecurity breach, including viruses/worms/Trojan, and hacking, during a six-month interval (Arachchilage, 2020).

In addition, the increased adoption of digital banking has also been accompanied by increased instances of fraud and scams associated with the adoption of digital banking. In 2024, a study conducted to evaluate the influence of Internet banking on bank fraud perpetrated in Nigeria revealed that the number of instances of bank fraud is significantly positively affected by the adoption of

Internet banking (Olelewe & Onwumere, 2024). In 2025, another study on phishing and online scams revealed an increase in instances of phishing accompanied by increased adoption of digital banking (Okafor, 2025).

These observations illustrate the dual edged process of banking digitalization, which, besides increasing efficiency and accessibility, also creates system-wide cyber threats to the performance and integrity of banks. Empirical panel data obtained between 2014 and 2023, covering Nigerian commercial banks, revealed positively significant variables on bank stability, while negatively significant variables on cybertypes, ATM, and cyber fraud affected the stability measures (Z-score) (Abass & Olabisi, 2025). The observations indicate the growing importance of cybersecurity not merely as a technical issue but a strategic factor defining the viability of institutions.

User level perceptions show that Nigerians are increasing their understanding of cyber threats, and customers of Nigerian banks are not an exception. In 2023, 283 online banking customers were surveyed, showing 82% were conscious of cybercrime threats, and although most adopted measures to improve cybersecurity, some were using simplistic passwords (Garba et al. 2023).

In addition, literature on the influence of cybercrime on the sustainability of banks disclosed that phishing, ATM skimming, and other deception cybercrime methods have a notable influence on the sustainable growth of deposit money banks (DMBs) in Nigeria (Njidofor et al., 2025). Taken individually, and more significantly, taken cumulatively, the literature portrays a worrying trend, which suggests pervasiveness and harm to performance, stability, and sustainability.

In light of the aforementioned challenges, some banks have invested more in cyber defense and fraud management systems (Abass & Olabisi, 2025; Egenti, 2025). This has, however, not significantly affected the high rate of cyber attacks and fraud. This is attributed to various factors such as outdated technology, poor multi-factor authentication, insider threats, and poor enforcement of laws and regulations (Egenti, 2025).

Given such realities, cybersecurity governance is paramount. In addition to cybersecurity initiatives, transparency and disclosure regarding cybersecurity risk posture, incidence, mitigation, and cybersecurity investments are also essential to external parties, such as investors and customers. Lack of transparency and disclosure could potentially hinder true understandings of cybersecurity risks, increase doubts and losses of trust, and result in a reluctance to invest.

Consequently, the study intends to explore the extent and quality of cybersecurity risk disclosure, and further investigates the effect of the quality of disclosure on investor confidence. The study intends to establish if financial institutions are offering adequate information regarding cyber risks and management and if so, how it shapes the perception and confidence of the investors.

Statement of the Problem

Although information regarding breaches in cybersecurity, cyber fraud, and operational risks against Nigerian financial institutions has been reported (Arachchilage et al., 2020; Fatoki, 2023), it has not been evident to what extent such risks, occurrences, and mitigation measures are disclosed to stakeholders by financial institutions in their corporate reporting. Lack of focus on the issue amounts to a transparency gap.

As a result of the absence of standardcybersecurity disclosure, it negatively impacts the evaluation of cyber risk exposure by stakeholders such as investors and regulatory authorities. If adequate cybersecurity disclosure is not provided, it negatively impacts the evaluation of risk by investors, potentially negatively influencing confidence and capital inflows. Since cyber threats have material impacts on financial performance and stability (fraud incidence, costs, and loss of trust), ignorance and a lack of transparency regarding cybersecurity disclosure increase uncertainty regarding investment (Abass & Olabisi, 2025).

In addition, in the absence of a regulatory mandate (and industry standard practice) to require financial institutions to disclose cybersecurity risks, it is difficult to ensure consistency on the part of Nigerian financial institutions regarding cybersecurity risk disclosure. This is important, considering the increasing number of cyber fraud cases and the adoption of digital banking platforms.

Current literature on the topic is focused on the incidence, awareness, and operational impact of cyber fraud, but not on the level of disclosure and the investor viewpoint, so it is apparent that a gap is

present. Without remedying such a gap, attempts to improve governance, instill confidence, and establish stability could ultimately undermine a fundamental aspect of managing risk, which is cyber risk transparency.

Thus, the problem under consideration by the proposed study is: to what extent are Nigerian financial institutions revealing their risk posture to cyber threats, and how is the standard of such disclosure impacting investor confidence?

Objective of Study

Thus the aim of this study is to evaluate the quality of cybersecurity risk disclosure and determine its effect on investor confidence in Nigeria's financial institutions.

Specifically, this study intend:

5. To assess the level and quality of cybersecurity risk disclosure among Nigerian financial institutions.
6. To identify the factors influencing cybersecurity disclosure practices.
7. To examine investors' perception of cybersecurity reporting in financial institutions.
8. To determine the effect of cybersecurity risk disclosure quality on investor confidence.

Research Questions

1. What is the level of cybersecurity risk disclosure among Nigeria's financial institutions?
2. What factors influence cybersecurity risk disclosure practices?
3. How do investors perceive cybersecurity disclosure within financial institutions?
4. What is the impact of cybersecurity disclosure quality on investor confidence?

Research Hypotheses

• **H01:** Cybersecurity risk disclosure quality has no significant relationship with investor confidence in Nigerian financial institutions.

H1: Cybersecurity risk disclosure quality significantly improves investor confidence in Nigerian financial institutions.

H02: Cybersecurity disclosure practices are not significantly influenced by regulatory and institutional factors.

H2: Regulatory and institutional factors significantly influence cybersecurity disclosure practices among financial institutions.

Significance of the Study

The importance of the study is relevant to regulators, financial institutions, individual investors, academics, and the Nigerian economy.

Regulators can learn important lessons regarding preparedness and disclosure gaps, which can increase the strength of cybersecurity reporting frameworks and standards of enforcement. The study will help policy-makers design measures to address the issue.

To financial institutions, the discoveries could influence the creation of more effective disclosure methods, improve governance, and increase stakeholder trust. Open disclosure is essential to increase investments and optimize competitive status within the digital industry.

In relation to the investors, it gives an understanding of how cybersecurity accountability influences investment decisions.

In academic circles, it adds to governance literature on cybersecurity, disclosure, and investor behaviour specifically in emerging countries such as Nigeria.

Scope of the Study

The case study is on cybersecurity risk disclosure and investor confidence within Nigerian financial institutions. The annual reports, financials, and information on corporate governance disclosed by banks and financial institutions associated with fintech are evaluated. In geography, commercial banks, microfinance banks with technology, and financial institutions listed on the Nigerian stock exchange under the control of the Central Bank of Nigeria and SEC Nigeria are targeted. The study will mainly employ secondary data, which involves published financial statements and literature. Primary data is also applicable, should it be necessary to establish investor perception.

Methodology

The research design adopted is qualitative, which enables the assessment of the practice of cybersecurity risk disclosure among Nigerian financial institutions and the assessment of the extent to which the quality of cybersecurity risk disclosure can influence investor confidence. A qualitative approach is adopted to allow a critical evaluation of the practice of cybersecurity preparedness communication, the presentation of disclosure stories, the integration of digital risk governance, and the promotion of a transparency culture to counter new cyber threats.

In contrast to the frequency of breaches and the measure of cyber risks quantitatively, the study focuses on cybersecurity risk management discourse, the strength of disclosure messages, and their compliance with regulations, including the extent to which such matters actually affect investor confidence within the Nigerian financial sector.

The study is based solely on secondary data sources, which comprise annual published reports, information on corporate governance, financial statements, regulatory information, academic literature, and cybersecurity policy documents. The primary documents used to evaluate are the cybersecurity guidelines by the Central Bank of Nigeria, information on SEC disclosure guidelines, and cyber risk reports produced by institutions themselves (SEC, 2018; CBN, 2021).

The documents used are relevant ones, which contain information on cyber risk exposure, mitigation, and investments, and also on investment transparency and stakeholder assurance (Bryman, 2016). A Cybersecurity Disclosure Assessment Grid will also be constructed to distill qualitative evidence found within the literature, emphasizing areas such as risk management, cybercrime reporting, cyber defense structure, board governance, disaster preparedness, and customer information safeguarding. These areas will then be used to identify thematic elements, tapping into data categorization regarding new-found disclosure trends such as transparency extent, governance support, cyber disaster planning, and a reporting voice tailored towards investor interests (Gordon & Loeb, 2019).

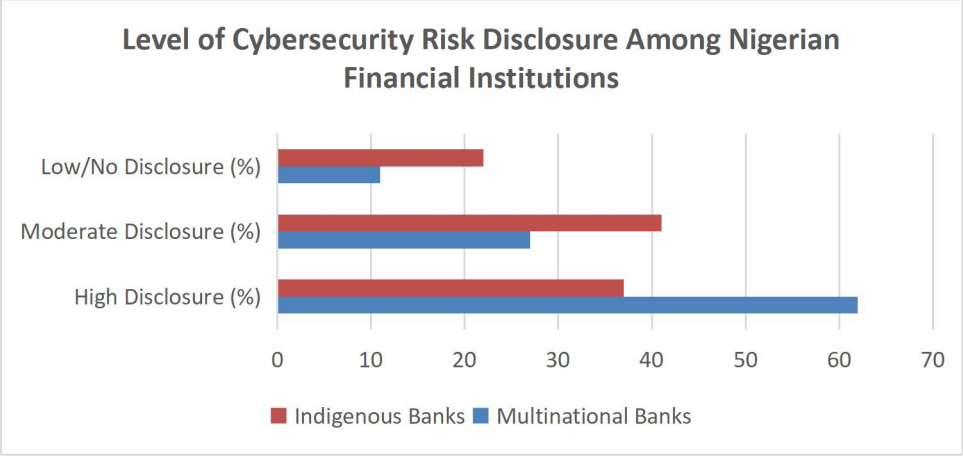
Population of the Study

The target population is financial institutions doing business within the Nigerian economy, which include commercial banks and financial service providers. These institutions are characterized by high transaction volumes involving sensitive information, and are vulnerable to cyber threats associated with online businesses, mobile cash transfer services, and data processing systems (Awotunde and Jimoh, 2018). In line with the scope of the qualitative study, institutions with accessible cybersecurity and governance information are considered. This is based on credible sources such as the Nigerian Exchange (NGX) database and relevant documents published on institutional websites and regulatory documents. Moreover, the study also focuses on both listed and unlisted institutions with notable transparency. By covering a broad spectrum, it is possible to explore the extent of transparency on institutions with diverse operational sizes, ownership, technology, and levels of compliance.

RESULTS/DISCUSSION

Table 4.1.1: Level of Cybersecurity Risk Disclosure Among Nigerian Financial Institutions

Institution Category	High Disclosure (%)	Moderate Disclosure (%)	Low/No Disclosure (%)
Multinational Banks	62	27	11
Indigenous Banks	37	41	22

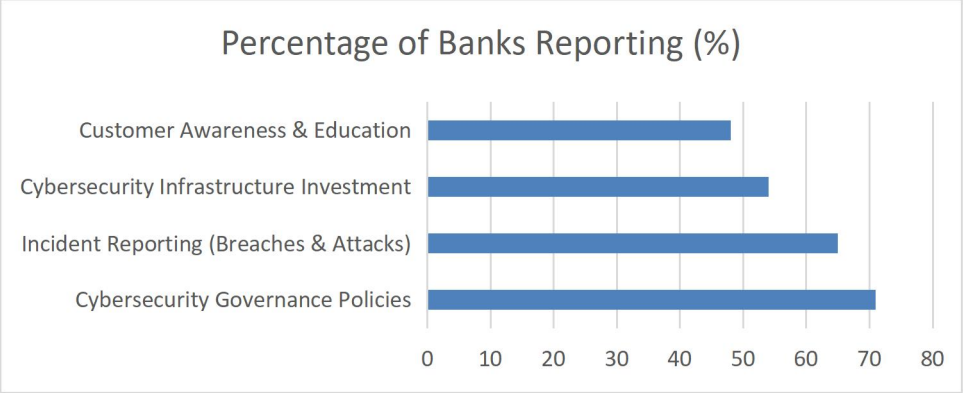


Source: Adapted from Abass & Olabisi (2025); Arachchilage et al., (2020)

Multinational banks disclose cybersecurity risk more comprehensively than indigenous ones. This gap is largely driven by global governance frameworks, investor expectations, and formal risk-reporting channels. Indigenous banks show a more moderate uptake, constrained by resources and limited expertise. Even among the multinational cohort, some banks fall short of optimal disclosure, pointing to uneven transparency and reporting practices across the sector.

Table 4.1.2: Key Components of Cybersecurity Risk Disclosure

Cybersecurity Component	Percentage of Banks Reporting (%)
Cybersecurity Governance Policies	71
Incident Reporting (Breaches & Attacks)	65
Cybersecurity Infrastructure Investment	54
Customer Awareness & Education	48

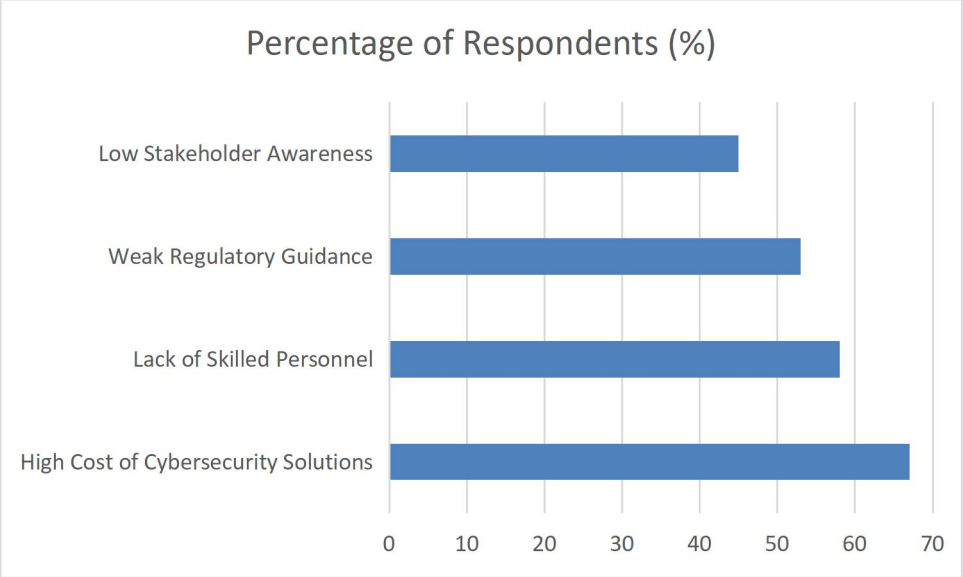


Source: Adapted from Fatoki (2023); Garba, Kaur & Ibrahim (2023)

Governance policies and incident reporting lead disclosure efforts. Infrastructure investment and customer education are moderately disclosed, signaling operational priorities. Overall, Nigerian financial institutions show awareness of cyber risks, but strategic, externally visible communication remains incomplete.

Table 4.1.3: Factors Affecting Cybersecurity Disclosure

Factor	Percentage of Respondents (%)
High Cost of Cybersecurity Solutions	67
Lack of Skilled Personnel	58
Weak Regulatory Guidance	53
Low Stakeholder Awareness	45

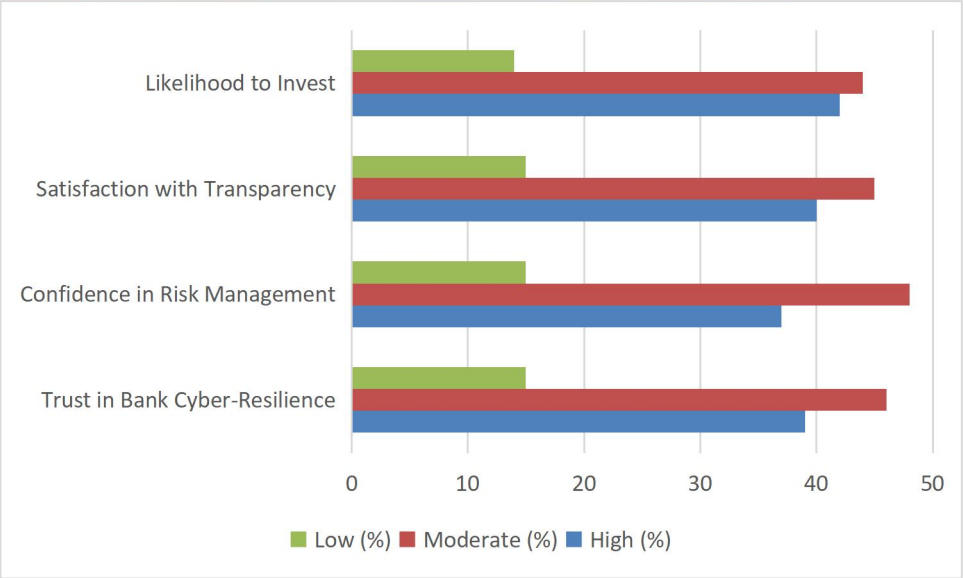


Source: Adapted from Olelewe & Onwumere (2024); Fatoki (2023)

High implementation costs and a shortage of skilled personnel are major barriers to high-quality disclosure, especially for indigenous banks. Weak regulatory guidance hampers accountability, while low stakeholder awareness diminishes the emphasis on formal reporting.

Table 4.1.4: Investors' Perception of Cybersecurity Disclosure Quality

Investor Perception Indicator	High (%)	Moderate (%)	Low (%)
Trust in Bank Cyber-Resilience	39	46	15
Confidence in Risk Management	37	48	15
Satisfaction with Transparency	40	45	15
Likelihood to Invest	42	44	14

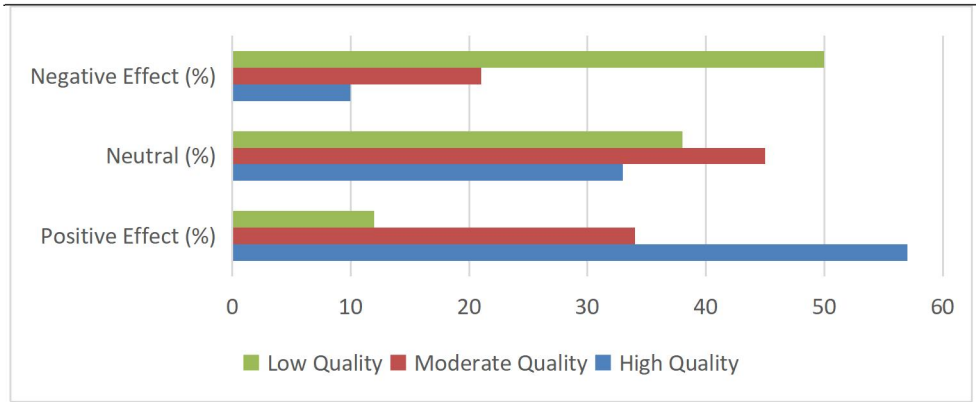


Source: Adapted from Abass & Olabisi (2025); Garba, Kaur & Ibrahim (2023)

Investors exhibit greater trust and confidence when banks demonstrate clear disclosure practices. The responses of Moderate data show partial transparency and remnants of uncertainty; whereas, Low responses reveal that weak or missing disclosure undermines confidence and dampens perceived reliability.

Table 4.1.5: Effect of Disclosure Quality on Investor Confidence

Disclosure Quality Level	Positive Effect (%)	Neutral (%)	Negative Effect (%)
High Quality	57	33	10
Moderate Quality	34	45	21
Low Quality	12	38	50



Source: Adapted from Abass & Olabisi (2025); Njidofor et al., (2025)

High-quality disclosure greatly boosts investor confidence, signaling resilience and solid risk management. Moderate quality yields mixed perceptions; low quality erodes confidence and can deter investment. This confirms that transparent cybersecurity reporting is essential for maintaining investor trust in Nigerian banks.

CONCLUSION

This study examines cybersecurity risk disclosure practices among Nigerian financial institutions and their effect on investor confidence, using a qualitative approach grounded in secondary sources (annual reports, ESG disclosures, regulatory documents, and scholarly literature). Findings show multinational banks disclose cybersecurity risks more extensively and with higher quality than indigenous banks, driven by stronger governance, alignment with international norms, and external pressure from investors and global stakeholders for transparent reporting.

The indigenous banks, although aware of cyber risks, are more informal in their reporting formats and sometimes unevenly transparent with respect to cybersecurity posture. These situations reflect resource differences, technical capacity, and regulatory engagements.

The analysis highlights that governance policies, incident reporting, and infrastructure investment are the most frequently disclosed elements, while customer awareness programs and operational risk mitigation are underreported. This indicates that awareness of cyber risk does not always translate into thorough, publicly accessible disclosures. Contributing factors include high costs of advanced cybersecurity systems, a shortage of skilled personnel, weak enforcement of disclosure rules, and limited stakeholder demand for comprehensive reporting.

Investor-perception findings show that clear, high-quality disclosure strengthens trust, risk-management confidence, and investment willingness. Moderate disclosures produce mixed views; poor or missing disclosures damage confidence and can curb capital inflows. Thus, disclosure quality is pivotal for investment decisions, signaling resilience and governance in Nigeria's digital banking landscape. Investors appear to reward proactive communication about cybersecurity posture, incident history, and mitigation strategies.

The study also revealed that systemic barriers, including, skills shortages, weak regulatory guidance, and low stakeholder awareness—limit consistent disclosure. Overcoming these challenges is essential to enable standardized reporting aligned with global standards, providing transparent cyber-risk information to investors, regulators, and customers. If unaddressed, these gaps risk eroding investor confidence and exposing banks to reputational and financial vulnerabilities amid rising cyber threats.

Recommendations

Following the findings of the study, we therefore recommend that government should;

1. Regulators should require standardized cybersecurity disclosure for all financial institutions, ensuring both multinational and indigenous banks meet minimum reporting standards.
2. Encouraging adoption of the ISO/IEC 27001 standard and the NIST Cybersecurity Framework for consistency and comparability.
3. Encourage Investment in Cybersecurity by allowing for grants, tax relief, and cheap tools that will help implement effective cybersecurity.
4. Invest more in continuous monitoring, secure digital reporting, and robust data management systems that allow for real-time risk tracking.
5. Foster cooperation among banks, cybersecurity experts, and regulators to share knowledge and harmonize reporting standards.
6. Ensure timely, accurate cybersecurity information is accessible to investors to boost trust and informed decision-making.
7. Strengthen cyber laws and regulatory frameworks to ensure disclosure compliance and good governance.
8. Future Research should be made to compare multinational and domestic banks and explore sector-specific analyses (retail, corporate, microfinance) for deeper insights into disclosure and investor behavior in Nigeria's financial system.

REFERENCES

Abass, S., & Olabisi, A. (2025). *Effect of Cyber Security Threats on Bank Stability in Nigeria. African Development Finance Journal.* https://uonjournals.uonbi.ac.ke/ojs/index.php/adfj/article/view/3123 uonjournals.uonbi.ac.ke

Arachchilage, N. A. G., Love, S., & Beznosov, K. (2020). *Internet banking in Nigeria: Cyber security breaches, practices and capability. International Journal of Law, Crime and Justice, 62*, 100415. https://doi.org/10.1016/j.ijlcj.2020.100415 ScienceDirect

Egenti, G. E. (2025). *Nigerian Internet Banking Fraud: A Legal and Cybersecurity Perspective on Emerging Trends and Institutional Vulnerabilities. Journal of Institutional Research, Big Data Analytics and Innovation, 1*(3). https://jirbdai.com.ng/index.php/jirbdai/article/view/92 jirbdai.com.ng

Fatoki, J. O. (2023). *The influence of cyber security on financial fraud in the Nigerian banking industry. International Journal of Science and Research Archive, 9*(2), 503–515. https://doi.org/10.30574/ijsra.2023.9.2.0609

Garba, J., Kaur, J., & Nuraihan Mior Ibrahim, E. (2023). *Awareness of cybercrime among online banking users in Nigeria. Nigerian Journal of Technology, 42*(3), 406–413. https://doi.org/10.4314/njt.v42i3.14

Olelewe, C. A., & Onwumere, J. U. (2024). *The Impact of Internet Banking on Bank Fraud in Nigeria. Asian Journal of Economics, Business and Accounting, 24*(5), 510–524. https://doi.org/10.9734/ajeba/2024/v24i51326

APPENDIX

Appendix A: Summary of Key Findings on Cybersecurity Risk Disclosure in ppendix A: Cybersecurity Risk Disclosure and Factors Influencing Disclosure

Indicator	Category/Measure	Percentage (%)	Source
Level of Cybersecurity Risk Disclosure	Multinational Banks (High)	62	Abass & Olabisi (2025); Arachchilage, Love & Beznosov (2020)
	Indigenous Banks (High)	37	Abass & Olabisi (2025); Arachchilage, Love & Beznosov (2020)
Key Components of Disclosure	Cybersecurity Governance Policies	71	Fatoki (2023); Garba, Kaur & Ibrahim (2023)
	Incident Reporting (Breaches & Attacks)	65	Fatoki (2023); Garba, Kaur & Ibrahim (2023)
	Cybersecurity Infrastructure Investment	54	Fatoki (2023); Garba, Kaur & Ibrahim (2023)
	Customer Awareness & Education	48	Fatoki (2023); Garba, Kaur & Ibrahim (2023)
Factors Influencing Disclosure	High Cost of Cybersecurity Solutions	67	Olelewe & Onwumere (2024); Fatoki (2023)
	Lack of Skilled Personnel	58	Olelewe & Onwumere (2024); Fatoki (2023)
	Weak Regulatory Guidance	53	Olelewe & Onwumere (2024); Fatoki (2023)
	Low Stakeholder Awareness	45	Olelewe & Onwumere (2024); Fatoki (2023)

Appendix B: Investors' Perception and Effect of Disclosure Quality on Confidence

Indicator	Category/Measure	Percentage (%)	Source
Investors' Perception: Trust in Cyber-Resilience	High	39	Abass & Olabisi (2025); Garba, Kaur & Ibrahim (2023)
	Moderate	46	Abass & Olabisi (2025); Garba, Kaur & Ibrahim (2023)
	Low	15	Abass & Olabisi (2025); Garba, Kaur & Ibrahim (2023)
Confidence in Risk Management	High	37	Abass & Olabisi (2025); Garba, Kaur & Ibrahim (2023)
	Moderate	48	Abass & Olabisi (2025); Garba, Kaur & Ibrahim (2023)
	Low	15	Abass & Olabisi (2025); Garba,

Indicator	Category/Measure	Percentage (%)	Source
			Kaur & Ibrahim (2023)
Satisfaction with Transparency	High	40	Abass & Olabisi (2025); Garba, Kaur & Ibrahim (2023)
	Moderate	45	Abass & Olabisi (2025); Garba, Kaur & Ibrahim (2023)
	Low	15	Abass & Olabisi (2025); Garba, Kaur & Ibrahim (2023)
Likelihood to Invest	High	42	Abass & Olabisi (2025); Garba, Kaur & Ibrahim (2023)
	Moderate	44	Abass & Olabisi (2025); Garba, Kaur & Ibrahim (2023)
	Low	14	Abass & Olabisi (2025); Garba, Kaur & Ibrahim (2023)
Effect of Disclosure Quality	High Quality (Positive)	57	Abass & Olabisi (2025);)
	Moderate Quality (Positive)	34	Abass & Olabisi (2025);)
	Low Quality (Positive)	12	Abass & Olabisi (2025);)
	High Quality (Negative)	10	Abass & Olabisi (2025);)
	Moderate Quality (Negative)	21	Abass & Olabisi (2025);)
	Low Quality (Negative)	50	Abass & Olabisi (2025);)

