http://journals.uonbi.ac.ke/index.php/adfj
ISSN 2522-3186

African Development Finance Journal
November Vol 8 No.9, 2025 PP 20-41
http://journals.uonbi.ac.ke/index.php/adfj
ISSN 2522-3186

Effect of Cyber Security Threats on Bank Stability in Nigeria

By: Dr Shiro Abass[1] and Adeoti Olabisi[2]

Abstract

This study examined the influence of cyber security risks on stability of banks in Nigeria. The main objective of the research work is to determine the impact of cyber security investments expenditure, fraud incidences and bank size variables on financial stability of Nigerian banks as measured using the Z-score. The study adopts a quantitative research design using panel data from 10 listed banks in Nigeria for the period 2014-2023. Data were analyzed by random effects regression, and to establish the correct model the Hausman test was performed. The results show that cyber security investment has significant positive effect on bank stability, and cyber security attacks, ATM fraud and cyber fraud have significant negative effect on stability. Interestingly, mobile fraud was positively correlated with stability, probably because banks experiencing higher fraud had put greater fraud prevention measures into place. Bank size was found not to have a significant influence on stability. Based on these findings, the study recommends that Nigerian banks invest more in cyber security, intensify regulatory measures and improve the education of the public on fraud prevention. In addition, banks should work together to share cyber security best practices and threat intelligence, which can help to create a more resilient financial system. These initiatives will contribute to reducing risks, building consumer confidence and providing a stable environment for banks in the long run.

Keywords: *Cyber security threats, bank stability, fraud prevention, Nigeria, financial resilience.*

1. Introduction

Bank stability is the foundation of economic prosperity and any attacks on the stability of banks can have a far-reaching effect on the financial sector and the economy at large. In Nigeria, financial institutions are essential in promoting economic development, financial inclusion and service access. Yet, as the banking industry is quickly going digital, the security of the cyberspace has become a major issue that threatens the stability of Nigerian banks. The increased number of cyber-attacks has cast some doubt on whether financial institutions can ensure continuity in their operations, protect customer information and data, and whether their financial transactions are secure. The threat of cyber security (including data breaches, malware, and phishing) has been undermining the capacity of banks to retain customer confidence and in certain instances financial stability. Such risks are a direct threat to the stability of banks as they destabilize the operational basis of the financial system (Fatoki, 2023; Austin-Olowo, Anike, and Ailemen, 2023).

[1]*Department of Finance, University of Lagos, Nigeria, Email: ashiro@unilag.edu.ng*
[2]*Department of Finance, University of Lagos, Nigeria, Email: adeotibisi@yahoo.co.uk*

In the face of these emerging threats, Nigerian banks are compelled to redefine their strategies to guarantee the security of digital banking platforms and ensure the financial sustainability of their operations. While digital banking has increased financial inclusion and access to banking services (Oni, Japinye, Ifarajimi, & Olubowale, 2025), it has also left bank infrastructure more vulnerable, and this has been exploited by cyber criminals for fraudulent activities. Not only do these cyber security breaches create huge financial losses, but they also undermine consumer trust, further jeopardizing the stability of banks. It is because of the ongoing threat of cyber-attacks that there has been a reexamination of conventional banking practices and the creation of stronger cyber security systems designed to alleviate such threats (Oyewole, Okoye, Ofodile, & Ugochukwu, 2024). In this context, it is essential to comprehend the impact of cyber security threats on the stability of Nigerian banks and, thus, sustain a resilient and secure financial landscape.

Cyber security risks are not just operational in nature, they are regulatory and governance challenges as well. The regulatory agencies in Nigeria have rolled out different systems to protect financial institutions from the growing menace of cybercrime. However, according to Cele and Kwenda (2025), there is a delicate balance between having strict cyber security regulations and facilitating financial inclusion, as overly restrictive measures may impede the adoption of digital financial services. Thus, in this Nigerian setting, where financial innovation and the regulatory oversight play a critical role in mitigating the risks of cyber threats, the intersection of cyber security regulation and bank stability is of paramount importance.

Strong governance frameworks play a crucial role in making a bank more resilient to cyber security risks. Banks with maturity in cyber security governance are better positioned to effectively manage risk and ensure that breaches do not lead to crisis situations (Elsayed, Ismail, & Ahmed, 2024). Institutionalized information security structures such as cyber security committees and risk management processes allow banks to be alert and proactive in meeting new threats. In spite of the advancement of cyber security management, there are few challenges that still remain for Nigerian banks regarding the adoption of robust cyber security strategies in response to the rapid advancement of technology and the tactics of cybercriminals (Opuni-Frimpong, Adefunso Dzorka, & Boadi, 2025).

Thus, the effects of cyber security threats on the Nigerian banks' economy go beyond the immediate financial loss to long-term impacts on profitability, market competitiveness, and customer retention. As the bank industry in Nigeria keeps on allocating enormous assets to cyber security frameworks, the expenditure connected to the network needs to be measured against the likelihood of business interruptions, reputational harm, and legal obligations (Wang, Asif, Shahzad, & Ashfaq, 2024). As such, a bank's capability to ensure a stable financial base in the face of these cybersecurity threats will be an important factor in their long-term viability in a competitive and highly dynamic market.

1.2 Research Problem

The rapid digital transformation in the Nigerian banking sector has introduced significant vulnerabilities in the form of cyber security risks, including data breaches, malware, and phishing attacks. These threats not only jeopardize the integrity of financial transactions but also undermine consumer trust, which is critical for the stability of banks. As Nigerian banks continue to prioritize digital banking to promote financial inclusion and economic development, they face the growing challenge of balancing technological innovation with robust cyber security measures. While investments in cyber security have increased, the rising number of cyber-attacks casts doubt on whether banks can effectively protect sensitive customer data, ensure the continuity of operations, and maintain financial stability in an increasingly digitized environment.

Moreover, despite the regulatory efforts in place, cyber security risks remain a persistent challenge for Nigerian banks. Regulatory bodies have implemented frameworks to mitigate the risks posed by cyber threats, yet there is a delicate balance between implementing stringent regulations and fostering financial innovation. Banks' ability to manage cyber security governance is crucial, but many face difficulties in adopting comprehensive cyber security strategies due to rapidly evolving technologies and the sophisticated tactics of cybercriminals. As a result, the problem lies not only in the immediate financial losses caused by cyber-attacks but also in the long-term impact on the profitability, competitiveness, and sustainability of Nigerian banks. This research aims to investigate how cyber security threats, alongside investment in cyber security measures, affect the stability of Nigerian banks.

1.3 Research Objectives

The following are the specific objectives

(a) To examine the impact of cyber security investment on bank stability.
(b) To explore the relationship between cyber security attacks and bank stability.
(c) To analyze the effect of mobile fraud on bank stability.
(d) To assess the influence of ATM fraud (ATMF) on bank stability.
(e) To evaluate the combined effects of cyber security investment, cyber security attacks, mobile fraud, and ATM fraud on bank stability (Z-score).

2. Literature Review

2.1 Theoretical Framework

2.1.1 Agency Theory

Agency Theory was developed by Michael Jensen and William Meckling in 1976 to explain the relationship between principals (shareholders) and agents (managers) in organizations. The theory argues that conflicts of interest can arise when managers prioritize their own utility (e.g., bonuses, career growth) at the expense of shareholders' long-term interests. These conflicts generate "agency costs," which must be minimized through governance mechanisms such as monitoring, incentive alignment, and transparent reporting. In the context of Nigerian banks, cyber security underinvestment is a typical agency problem. Managers may under-allocate resources to cyber security infrastructure because the costs are immediate, while the benefits are uncertain or long-term. This weakens bank resilience and exposes institutions to cyber risks that compromise stability. Agency Theory is therefore relevant because it highlights how governance failures and misaligned incentives can leave banks vulnerable to cyber-attacks, emphasizing the importance of governance mechanisms such as cyber security committees and disclosure policies (Elsayed, Ismail, & Ahmed, 2024).

2.1.2 Systems Theory

Ludwig von Bertalanffy introduced Systems Theory in 1968 as a framework for understanding organizations as complex, interrelated systems rather than isolated units. The theory posits that the failure or disruption of one component within a system can have ripple effects on the entire system. Applied to the Nigerian banking sector, banks function as socio-technical systems comprising

human actors, technology, policies, and external stakeholders. A cyber security breach in one subsystem, such as IT infrastructure, can cascade into broader operational failures, service disruptions, and reputational damage. Moreover, the interconnectedness of Nigerian banks through digital payment networks and clearing systems means that a breach in one institution could potentially destabilize others. Systems Theory is highly relevant to this study as it underscores the systemic nature of cyber security risks and the need for integrated defense mechanisms that protect both individual banks and the wider financial ecosystem (Bruno, Pistolesi, & Teti, 2025).

2.1.3 Technology–Organization–Environment (TOE) Framework

Technology Organization Environment (TOE) is a model of organizational adoption of innovation suggested by Louis Tornatzky and Mitchell Fleischer in 1990. The three factors in the framework are the technological context (availability and sophistication of tools), the organizational context (resources, culture, managerial support) and the environmental context (competition, regulation and external pressures). When using the TOE framework to explain the adoption of cyber security technologies by Nigerian banks, the effect of technological change in the adoption of encryption and AI-based detection tools, organizational preparedness in budgetary allocation and staff development, and environmental demand on regulators and customers are considered. Indicatively, the cyber security policies of the Central Bank of Nigeria influence the environment, and the organizational need to provide secure digital platforms affects the decisions of clients. The relevance of the TOE framework is that it offers a holistic prism through which to analyze the way Nigerian banks implement cyber security practices and the effects of such practices on their stability (Oni, Japinye, Ifarajimi, & Olubowale, 2025; Cele & Kwenda, 2025).

2.2 Empirical Review

Ajibare and Oguntuase (2025) examined the multifarious interaction between cyber security threats and financial inclusion in Nigeria. The statistical data used were both reputable and relevant sources like Nigeria Electronic Fraud Forum (NeFF) and World Bank Development Indicator. The hypotheses of the study were strictly tested using three estimation tools Ordinary Least Squares (OLS), Two-Stage Least Squares (2SLS), and Generalized Method of Moments (GMM). Key findings challenged existing assumptions, revealing unexpected relationships between the threats of cyber security and financial inclusion. Contrary to the assumption of the past, a positive long-

term relationship between cyber security risk and the requirement of financial inclusion has been identified. Cyber security threat has a significant effect on the supply dimension of financial inclusion.

Analysis was carried out by Oni, Japinye, Ifarajimi and Olubowale (2025). These issues are becoming more urgent because of the growing reliance on financial technology (FinTech) companies in Nigeria, which have raised concerns regarding cyber security risks, regulatory intervention, consumer trust, systemic stability, and financial inclusion. The interaction between these variables is critical and will help analyze their nature, reduce the risks, and ensure that the client trusts digital financial services. This paper reviewed 248 responses of fintech users, regulators, and industry gurus through a stratified survey using stratified random sampling. The empirical study involved Structural Equation Modelling (SEM). Regulatory measures, consumer confidence, systemic resilience and financial inclusion are considered as latent variables and the underlying elements of cyber security risks are analyzed. Results revealed that cyber security threats play a significant role in regulatory actions, suggesting that the higher the vulnerability, the more the regulatory action was needed. The important role of financial market protection is highlighted because regulatory actions have a positive impact on consumer confidence and systemic stability. On the other hand, financial inclusion is adversely impacted by cyber security issues. In addition, regulatory interventions affect the correlation existing between cyber security threats and financial inclusion, which indicates that, although regulations enhance security, they tend to pose an unintentional barrier to financial inclusion. This study presents new information in the existing bodies of research regarding FinTech regulation, financial inclusion, and systemic resilience.

Opuni-Frimpong, Adefunso Dzorka, and Boadi (2025) examined the effect of the Bank of Ghana (BoG) decision to introduce a Cyber and Information Security Governance Committee (CISGC) on the financial performance (FP) and operational efficiency of banks. Bank financial performance is measured by the return on assets (ROA), and on equity (ROE), and efficiency is measured by the ratio of the operation cost on operating revenue (CIR). The report examines the cyber and IT expertise, committee structure, meeting frequency and the representation of females in the CISGC. The sample of 20 universal banks in Ghana between 2019 and 2022 was used to test the impact of

CISGC characteristics on the financial performance and efficiency of banks using generalized least squares regression and robustness testing. The cyber and IT knowledge of CISGC has a positive impact on ROA, but not on ROE or CIR. Neither their size nor their meetings nor their proportion of women affect performance.

Ama, Onwubiko, and Nwankwo (2024) examined cybersecurity issues in Nigerian deposit money banks (DMBs), emphasising the proactive strategies employed by both banks and customers to address these concerns. The research strategy utilises a descriptive methodology and census sample, gathering data from employees of designated DMBs using questionnaires. Data study utilizing SPSS revealed that the primary difficulties facing cyber security in banks include pharming, identity theft, SIM swap fraud, skimming/website cloning, and smishing/vishing. The primary issues identified included deficiencies in the banks' internal control systems, insider misconduct by bank personnel, and a lack of awareness and security consciousness among banking clients. Banks employ strategies include encryption, password modifications, and the banning of unsolicited mail to reduce cyber security threats.

Buraale, Abdurrahman, and Fauzi (2024) assessed the existing cyber security awareness among IT professionals in the banking and telecom sectors in Bosaso, aiming to identify significant weaknesses and risks facing these companies. A quantitative survey was executed, focusing on IT specialists within the banking and telecommunications industries of Bosaso. The poll evaluated participants' awareness of cyber security dangers, their confidence in current security measures, and their experiences with cyber events. Data were examined through descriptive statistics and thematic analysis to clarify prevalent themes and patterns. The poll indicated that although most IT professionals recognize prevalent cyber security dangers, there exists a considerable deficiency in trust regarding the sufficiency of existing security protocols. Identified key weaknesses encompass inadequate personnel training, obsolete software, and insufficient investment in modern security solutions. Additionally, 65% of participants indicated that they encountered at least one cyber incident in the previous year. These findings highlight the pressing necessity for improved cyber security measures.

Nwankwo, Kanyangale, Anoke, and Eze (2023) investigated the impact of cyber security on the commercial viability of three publicly listed and highly valued microfinance banks in Nigeria. The study population comprised 315 senior, mid-level, and junior staff from three microfinance banks in Nigeria. The research employed a census due to the manageable size of the target population. Data were gathered by a semi-structured questionnaire, and the proposed hypothesis was examined using multiple regression analysis. The research indicated that cyber security substantially and favorably influences the sustainability of microfinance banks in Nigeria. Data availability constitutes the most significant factor in the sustainability of MFBs, succeeded by data confidentiality and data integrity. Employees in a microfinance bank assert that data availability, confidentiality, and integrity are crucial components of cyber security that impact the sustainability of their companies in Nigeria.

Austin-Olowo, Anike, and Ailemen (2023) examined various cyber security challenges impacting online banking and transactions in Nigeria, aiming to enhance the resilience of the financial system against these systemic risks. The researcher utilized both primary and secondary data to investigate the historical and contemporary trends in cyber security impacting online banking and transactions. This research indicated that hacking into client accounts and delays in transferring funds between banks adversely affect internet banking and transactions in Nigeria.

Elsayed, Ismail, and Ahmed (2024) employed manual textual analysis to assess cyber security disclosures in a sample of publicly listed banks within MENA area countries, utilizing data from 2019 to 2021. The data were obtained from the annual reports and financial statements of banks accessible in the Orbis Bank Focus database. The research utilized a random effects regression model to evaluate the hypotheses and analyze the findings. The results indicate that banks in the MENA region are progressively inclined to provide cyber security information, with cyber security disclosure rising from 17% in 2019 to 19.6% in 2021. Furthermore, the findings indicate that cyber security disclosure exerts a favorable and significant impact on bank performance. The findings imply that the presence of a Chief Risk Officer moderates the association between cyber security disclosure and bank performance.

Wang, Asif, Shahzad, and Ashfaq (2024) examined the difficulties banks have in preserving data privacy and cyber security during the adoption of new technologies, their perceptions of these problems, and the measures they undertake to mitigate associated risks. This qualitative study use topic analysis to investigate interviews with IT specialists in the banking sector. NVivo 14 software is utilized to discern principal themes and patterns about the issues, perspectives, and tactics associated with data privacy and cyber security in technology adoption. The results indicate that the principal issues confronting banks encompass the integration of legacy systems, the evolution of compliance management, the management of vendor risks, the preservation of consumer confidence, and the mitigation of developing risks.

3. Research Methodology

3.1 Research Design

The study employed an ex-post facto research design. This design was considered appropriate because the data were secondary in nature, drawn from banks' annual reports, and could not be manipulated by the researcher. Ex-post facto research is widely used in financial and economic studies where historical data are analyzed to establish relationships among variables.

3.2 Population and Sample

The population of the study comprised all listed deposit money banks in Nigeria. From this population, 10 banks were purposively selected based on the availability and consistency of data reporting during the period under review. The study covered a ten-year period from 2014 to 2023, and data were extracted from the published annual reports of these banks.

3.3 Model Specification

To assess the effect of cyber security threats on bank stability in Nigeria, a multiple regression model was specified as follows:

$$Zit=\beta0+\beta1CINVit+\beta2CATTit+\beta3MOBFit+\beta4ATMFit+\beta5BSZit+\beta6CFRit+\mu it$$

Where:

Zit = Bank stability of bank *i* in year *t* (measured by z-score

CINV = Amount invested in cyber security (₦, natural log)

CATT = Frequency of reported cyber security attacks

MOBF = Mobile banking fraud incidents

ATMF = ATM fraud incidents

BSZ = Bank size (log of total assets)

CFR = General Cyber fraud cases

μit = Error term

Table 1: Variable Measurement and Expected Sign

Variable	Measurement/Proxy	Description	Expected Sign
Bank Stability (Z-score)	(ROA + Equity/Assets) ÷ σ(ROA)	Insolvency risk: higher values imply stronger bank stability	Dependent
Cybersecurity Investment (CINV)	Annual expenditure on cybersecurity (₦, log)	Reflects banks' financial commitment to protecting systems	Positive (+)
Cybersecurity Attacks (CATT)	Number of reported cybersecurity incidents	Captures exposure to external cyber threats	Negative (–)
Mobile Fraud (MOBF)	Number of reported mobile fraud cases	Fraud committed via mobile banking channels	Negative (–)
ATM Fraud (ATMF)	Number of reported ATM fraud cases	Fraudulent activities linked to ATM transactions	Negative (–)
Bank Size (BSZ)	Natural log of total assets	Proxy for economies of scale and resource base	Positive (+)
Cyber Fraud (CFR)	Number of cyber fraud cases	General digital-related fraud across platforms	Negative (–)

Source: Researchers Compilation (2025)

3.4 Method of Data Analysis

The study applied panel regression analysis, which combines cross-sectional and time-series data, making it suitable for evaluating variations across banks and over time. The analysis began with descriptive statistics to summarize the data in terms of mean, standard deviation, minimum, and maximum values. Correlation analysis was conducted to identify the degree of association among variables and check for possible multicollinearity issues.

To test the study's hypotheses, both fixed effects and random effects panel regression models were estimated. The Hausman specification test was then conducted to determine the more consistent and efficient estimator between the fixed effects and random effects models. If the Hausman test

was statistically significant ($p < 0.05$), the fixed effects model was adopted; otherwise, the random effects model was considered appropriate.

The decision rule for hypothesis testing was based on the probability value (p-value). At the 5% level of significance, if the p-value of a variable was less than 0.05, the null hypothesis of no significant relationship was rejected, indicating that the independent variable significantly influenced bank stability. Conversely, if the p-value exceeded 0.05, the null hypothesis was not rejected, suggesting that the variable did not have a statistically significant impact on bank stability.

4. Result and Discussion

4.1 Descriptive Analysis

Table 2: Summary of Descriptive Statistics

	Z_SCORE	CINV	CATT	MOBF	ATMF	CFR	BSZ
Mean	5.205	288.703	6.660	14.080	9.420	11.290	6.559
Median	5.196	276.706	6.000	14.000	9.000	10.000	6.451
Maximum	5.980	498.129	14.000	24.000	14.000	19.000	8.484
Minimum	4.508	102.235	1.000	5.000	5.000	5.000	4.629
Std. Dev.	0.446	111.446	4.023	6.201	3.059	4.604	1.165
Skewness	0.112	0.070	0.322	-0.009	0.107	0.183	0.071
Kurtosis	1.721	1.865	1.970	1.660	1.711	1.708	1.788
Jarque-Bera	7.022	5.448	6.152	7.482	7.114	7.508	6.201
Probability	0.030	0.066	0.046	0.024	0.029	0.023	0.045
Observations	100	100	100	100	100	100	100

Source: Researchers Computations (2025)

Table 2 presents the summary of descriptive statistics for key variables related to bank stability and cyber security threats. The Z-score, which measures bank stability, has a mean of 5.205, with a median of 5.196, indicating that most banks in the sample exhibit relatively high financial stability. The maximum value of 5.980 and the minimum value of 4.508 show that while there is some variation in stability across the banks, all remain within a stable range. The standard deviation of 0.446 suggests that there is limited fluctuation in the stability measures, with banks maintaining similar levels of stability. The skewness of 0.112 and kurtosis of 1.721 point to a nearly normal distribution, with minimal skew towards stability and a moderate peak, implying that most banks are clustered around the stable zone with only slight deviations.

For cyber security investment (CINV), the mean value of ₦288.703 million reflects substantial investment in cyber security by Nigerian banks. The standard deviation of ₦111.446 million indicates considerable variability in cyber security spending, with some banks making much higher investments than others. The skewness of 0.070 and kurtosis of 1.865 suggest that the data is relatively symmetric and slightly flatter than a normal distribution. The probability value of 0.066 suggests a marginal deviation from normality, but the difference is not significant enough to affect the robustness of the analysis.

Looking at cyber security attacks (CATT), the mean of 6.660 with a standard deviation of 4.023 shows that banks experience a moderate frequency of cyber-attacks, with considerable variation in the number of incidents across banks. The maximum of 14 and minimum of 1 indicate that while most banks report 5 to 7 incidents per year, a few banks are affected by more frequent breaches. The skewness of 0.322 points to a slight positive skew, suggesting that a few banks face much higher levels of attacks than the rest. The kurtosis of 1.970 suggests a distribution with heavy tails, meaning some banks are significantly more vulnerable to cyber-attacks than others. The probability value of 0.046 confirms that the distribution is significantly non-normal.

In the case of mobile fraud (MOBF), ATM fraud (ATMF), and cyber fraud (CFR), the mean values are 14.080, 9.420, and 11.290, respectively. These high averages indicate frequent incidents of fraud across the banks. The standard deviations of 6.201 for mobile fraud and 3.059 for ATM fraud show that there is substantial variation in the fraud levels reported by different banks. The relatively low skewness values for both variables indicate that most banks experience moderate to high fraud levels, but there are a few banks facing significantly higher levels of fraud. The bank size (BSZ), measured as the log of total assets, has a mean of 6.559 and a low standard deviation of 1.165, suggesting that there is less variation in bank size compared to the cyber security and fraud variables. Finally, the probability values for all variables being less than 0.05 indicate that their distributions significantly differ from normality, with some variables showing more pronounced skewness and kurtosis, reflecting the diverse nature of data related to the frequency and severity of cyber security threats and fraud incidents across the banks.

4.2 Correlation Analysis

Table 3: Correlation Matrix

	LZ_SCORE	LCINV	LCATT	LMOBF	LATMF	LCFR	BSZ
LZ_SCORE	1						
LCINV	-0.186	1					
LCATT	0.173	-0.095	1				
LMOBF	0.262	0.059	-0.005	1			
LATMF	-0.286	0.031	-0.067	-0.054	1		
LCFR	-0.256	-0.246	-0.035	0.113	0.025	1	
BSZ	-0.026	-0.244	-0.037	0.109	0.027	0.134	1

Source: Researchers Computations (2025)

The correlation analysis reveals several key relationships between the variables under study. The Z-score (which measures bank stability) shows a slight negative correlation with cyber security investment (CINV) (r = -0.186), suggesting that higher cyber security expenditures are weakly associated with lower bank stability. This could imply that banks facing higher cyber security risks may be compelled to spend more, yet still experience instability. Conversely, the Z-score is positively correlated with mobile fraud (MOBF) (r = 0.262), indicating that banks experiencing more mobile fraud incidents may have developed stronger resilience, contributing to greater stability. However, a negative correlation is observed between Z-score and both ATM fraud (ATMF) (r = -0.286) and cyber fraud (CFR) (r = -0.256), suggesting that higher incidents of these types of fraud are linked to decreased bank stability. Interestingly, the correlation between bank size (BSZ) and Z-score is negligible (r = -0.026), indicating that the size of the bank does not significantly affect its stability in the context of cyber security threats. Overall, these results highlight that while certain types of fraud negatively influence bank stability, the relationship between cyber security investment, bank size, and stability is less straightforward and requires further investigation.

4.3 Hausman test

Table 4: Hausman Test

Correlated Random Effects - Hausman Test			
Test Summary	Chi-Sq. Statistic	Chi-Sq. d.f.	Prob.
Cross-section random	1.947630	6	0.9245

Source: Researchers Computations (2025)

Table 4 presents the Hausman test results for the panel data regression. The Chi-Square statistic for the test is 1.947630 with 6 degrees of freedom, and the p-value is 0.9245. Since the p-value is greater

than 0.05, we fail to reject the null hypothesis. This indicates that the random effects model is more appropriate than the fixed effects model for this analysis, as there is no significant difference between the coefficients estimated by the fixed and random effects models.

4.4 Panel Regression

$$Zit=\beta0+\beta1CINVit+\beta2CATTit+\beta3MOBFit+\beta4ATMFit+\beta5BSZit+\beta6CFRit+\mu it$$

Table 5: Random Effect Regression

Cross-section random effects test equation:				
Dependent Variable: LZ_SCORE				
Method: Panel Least Squares				
Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	-5.558	4.530	-1.227	0.223
LCINV	1.420	0.622	2.285	0.031
LCATT	-1.045	0.512	-2.042	0.043
LMOBF	0.932	0.419	2.227	0.031
LATMF	-2.623	1.028	-2.551	0.018
LCFR	-9.287	4.314	-2.153	0.035
BSZ	-0.166	0.113	-1.471	0.145
	Effects Specification			
R-squared	0.624	Mean dependent var		0.715
Adjusted R-squared	0.582	S.D. dependent var		0.037
F-statistic	10.734	Durbin-Watson stat		1.970
Prob(F-statistic)	0.000			

Source: Researchers Computations (2025)

Table 5 shows the random effects regression results for the model examining the relationship between cyber security threats and bank stability. The dependent variable is Z-score (LZ_SCORE), a measure of bank stability, and the model includes several independent variables: cyber security investment (LCINV), cyber security attacks (LCATT), mobile fraud (LMOBF), ATM fraud (LATMF), cyber fraud (LCFR), and bank size (BSZ).

Cyber security Investment (LCINV): The coefficient of 1.420 ($p = 0.031$) is statistically significant at the 5% level, indicating a positive relationship with bank stability. This suggests that increased cyber security investment is associated with greater bank stability, which aligns with expectations that stronger security measures contribute to a more secure banking environment.

Cyber security Attacks (LCATT): The coefficient of -1.045 (p = 0.043) is significant at 5 per cent level implying a negative relationship with bank stability. This means that the higher the rate of cyber security attacks, the more the banks are likely to instability, perhaps because of the disruptive impact of cyber security attacks on business and customer confidence.

Mobile Fraud (LMOBF): Coefficients of 0.932 (p = 0.031) are significant (the 5% level) and indicate a positive correlation with bank stability. This finding implies that banks experiencing higher cases of mobile frauds may be investing in more robust fraud detection and prevention tools, which help to stabilize the situation.

ATM Fraud (LATMF): The coefficient of -2.623 (p = 0.018) is significant at the 5% level and represents a negative association with stability. The higher the ATM fraud incidents, the less stable the situation is, probably due to the reputational and operation costs involved in ATM fraud cases.

Cyber Fraud (LCFR): The correlation = -9.287 (p = 0.035) is significant at the 5% threshold, which is negative and, therefore, shows that bank stability is negatively correlated with this variable. The higher the number of cyber fraud cases a bank experiences, the less stable the bank is, which validates the claim that digital fraud erodes trust and security in financial institutions.

Bank Size (BSZ): The coefficient of -0.166 (p = 0.145) is not statistically significant, suggesting that bank size does not have a significant impact on stability in this context. This may indicate that bank size does not play a major role in the relationship between cyber security threats and bank stability.

The model explains approximately 62.4% of the variation in bank stability, as indicated by the R-squared value, with an adjusted R-squared of 58.2%. The F-statistic of 10.734 ($p < 0.001$) indicates that the model is statistically significant, suggesting that the independent variables collectively explain a meaningful portion of the variation in bank stability. The Durbin-Watson statistic of 1.970 indicates no serious autocorrelation issues in the residuals.

These results highlight the importance of cyber security measures and fraud management in enhancing bank stability, with certain types of fraud (e.g., cyber fraud, ATM fraud) significantly undermining bank performance.

4.5 Diagnostic Test

Table 6: Residual Cross-Section Dependence Test

Residual Cross-Section Dependence Test			
Null hypothesis: No cross-section dependence (correlation) in residuals			
Test	Statistic	d.f.	Prob.
Breusch-Pagan LM	3.200	45	0.1250
Pesaran scaled LM	2.973		0.2530
Pesaran CD	-0.739		0.4600

Source: Researchers Computations (2025)

Table 6 presents the results of the Residual Cross-Section Dependence Test, which tests whether there is cross-sectional dependence (i.e., correlation) in the residuals of the panel data model. The Breusch-Pagan LM statistic of 3.200 with a p-value of 0.1250 and the Pesaran scaled LM statistic of 2.973 with a p-value of 0.2530 both fail to reject the null hypothesis, suggesting that there is no significant cross-sectional dependence among the residuals. Similarly, the Pesaran CD statistic of -0.739 with a p-value of 0.4600 further supports this conclusion, indicating that the residuals are not correlated across the cross-sections. Therefore, the results suggest that there is no significant correlation between the errors across the banks, and the assumption of cross-sectional independence holds in this model.

4.6 Discussion of Findings

There is a positive, statistically significant relationship between Cyber security Investment and bank stability, and this relationship is 1.420 ($p = 0.031$). This observation suggests that banks with higher spending on cyber security have more stability, which is consistent with the assumption that proactive risk management with cyber security measures increases the resilience of banks. Enhanced cyber security spending, including enhanced encryption, better fraud-detection mechanisms, and data protection seems linked to better bank performance/stability. The finding is in line with that of Nwankwo et al. (2023), who have determined that cyber security is a major issue affecting sustainability of financial institutions in Nigeria. Although certain sections of the analysis demonstrate a slight negative correlation, the findings indicate that a business taking steps

to enhance its cyber security can reduce risk and build confidence in the bank responding to instances of digital threats, a factor that supports the overall stability.

On the other hand, Cyber security Attacks demonstrates an inverse relationship with bank stability with the coefficient of = -1.045 (p = 0.043). This result indicates that the high frequency of cyber security attacks is associated with a low level of stability among banks. The minus value of the coefficient is also large, which means that the more cyber-attacks the banks are subjected to, the lower the efficiency and reliability of their operations, thus they may become unstable. This finding reinforces prior studies by Oni et al. (2025), who concluded that escalated cyber security vulnerabilities drive the necessity to undertake a regulatory response in the name of maintaining financial stability. Cyber security attacks damage the confidence of customers, interrupt financial business, and raise the recovery cost, which affect the stability of the bank adversely. The inverse connection in this report underlines the urgency of banks to enhance their fortifications and engage in proactive approaches to security measures to reduce the disruption impacts of cyber threats.

Mobile Fraud is positively correlated with Z-score (coefficient = 0.932, p = 0.031), which implies that an increase in mobile fraud events is accompanied by increased bank stability. It may not sound intuitive initially, but that may be an indication of the proactive efforts of the banks to address mobile fraud, including implementation of high-tech fraud detection solutions, greater attention to transactions, and communication with customers. Banks with a higher number of mobile fraud cases might be dedicating additional capital to technology and security infrastructure to secure their systems and this can create better overall stability. This is in line with the results obtained by Ajibare and Oguntuase (2025), who found a positive connection between cyber security threats and financial inclusion, which may indicate the effectiveness of resilience and security as solutions to the new challenges of fraud.

There is a negative correlation between ATM Fraud and Z-score as well as Cyber Fraud and Z-score with coefficients of -2.623 (p = 0.018) and -9.287 (p = 0.035) respectively. This shows that the less ATM fraud and cyber fraud cases are reported, the less the stability of the banks. These types of fraud result in financial losses, reputational damage, and rising costs of operations which all contribute to a lack of stability. This observation supports the results of Oyewole et al. (2024),

who reported that cyber security attacks, and especially those of scam nature, have a direct impact on the stability of financial institutions, eroding customer trust and leading to inefficiency. The negative correlation highlights the significance of strong cyber security systems to curb and alleviate the effects of such forms of fraud, which continue to be on the rise in the digital banking landscape.

Finally, there is a weak correlation between Bank Size and bank stability (coefficient = -0.166, p = 0.145), and this indicates that the size of a bank does not play a significant role in determining its capacity to overcome cyber security threats. Although bigger banks tend to have greater resources and infrastructure, this study reveals that elements like investment in cyber security and managing fraud are more important determinants of stability. It is not the first study to find this, with Fatoki (2023) also suggesting that the size of a bank may offer certain benefits, but the attitude of this bank toward its cyber security and risk management has a more significant influence on its stability.

5. Conclusion and Policy Recommendations

5.1 Conclusion

The paper examines how cyber security threats influence the stability of banks in Nigeria based on the important variables of cyber security investment, fraud type, and bank size. The results indicate that cyber security investment is a key indicator of improving the stability of the bank, whereas cyber security attacks and other types of fraud, especially ATM fraud and cyber fraud, lead to a negative impact on the stability of the bank. The study also established positive correlation between mobile fraud and bank stability, which implies that the more mobile fraud cases banks have, the more robust measures they apply to protect their operation, thereby enhancing resilience. Although the effect of bank size on stability is insignificant, the findings highlight the importance of banks focusing on sound cyber security policies to ensure the stability and operational integrity of the bank system in the presence of changing cyber threats. The study adds value to the existing literature on the banking industry in terms of cyber security due to the intricate nature of interrelations between cyber threats and financial stability. The results shed more light on the relation between investment in cyber security and the rate of fraud cases and the stability of Nigerian banks as this is essential to the policymakers and banking institutions.

5.2 Policy Recommendations

(i) Since there is a positive correlation between the investment in cyber security and the stability of banks, the policy makers should incentivize the Nigerian banks to invest more in cyber security. Banks must focus on investing in complex fraud detection software and encryption tools as well as employee training programs.

(ii) The adverse effects of cyber security attacks on stability make the tighter regulation of the issue more crucial. Stricter cyber security rules should be enforced by regulatory bodies and banks should be subjected to industry standards. Cyber security audits and vulnerability assessments should be required on a regular basis to highlight and mitigate potential risks before they become severe.

(iii) The banks and the regulators should join hands in conducting awareness campaigns to the masses on the dangers of fraud and how to use their bank safely. Training customers on recognizing fraud, sim-swapping and other types of phishing can significantly reduce the cases of mobile fraud and aid in overall cyber security.

(iv) Since cyber security threats are not often specific to one bank, banks can also participate in industry wide activities sharing threat intelligence and best practices. It can collaborate with other financial institutions and other international cyber security bodies to make the banking system more resilient.

References

Ajibare, A. O., & Oguntuase, O. J. (2025). Cyber security Threats and Their Impact on Financial Inclusion Drivers in Nigeria. *London Journal*, 449, 449U.

Alsakini, S. A. K., Alawawdeh, H. A., & Alsayyed, S. (2024). The impact of cyber security on the quality of financial statements. *Appl. Math*, 18(1), 169-181.

Ama, G. A. N., Onwubiko, C. O., & Nwankwo, H. A. (2024). Cyber security Challenge in Nigeria Deposit Money Banks. *Journal of Information Security*, 15(4), 494-523.

Austin-Olowo, L. B. A., Anike, O. I., & Ailemen, I. O. (2023). Cyber security issues affecting online banking and transactions in Nigeria. *International Journal of Arts, Languages and Business Studies*, 9, 25-35.

Bruno, E., Pistolesi, F., & Teti, E. (2025). Cyber security policy, ESG and operational risk: A Virtuous relationship to improve banks' performance. *International Review of Economics & Finance*, 99, 104053.

Buraale, M. A., Abdurrahman, T. K., & Fauzi, F. C. (2024). Assessing cyber security threats and awareness in bosaso's banking and telecom sectors. *International Journal of Science and Research (IJSR)*, 13(8), 738-747.

Cele, N. N., & Kwenda, S. (2025). Do cyber security threats and risks have an impact on the adoption of digital banking? A systematic literature review. *Journal of Financial Crime*, 32(1), 31-48.

Elsayed, D. H., Ismail, T. H., & Ahmed, E. A. (2024). The impact of cyber security disclosure on banks' performance: the moderating role of corporate governance in the MENA region. *Future Business Journal*, 10(1), 115.

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.

Kundavaram, R. R., Onteddu, A. R., Nizamuddin, M., & Devarapu, K. (2023). Cyber security Risks in Financial Transactions: Implications for Global Trade and Economic Development. *Global Disclosure of Economics and Business*, 12(2), 53-66.

Nwankwo, C., Kanyangale, M., Anoke, A. F., & Eze, S. U. (2023). Effect of cyber security on business sustainability of listed microfinance banks in Nigeria. *Artha Journal of Social Sciences*, 22(1), 79-106.

Oni, O., Japinye, A. O., Ifarajimi, G. D., & Olubowale, F. O. (2025). Regulating fintech for financial stability in Nigeria: balancing cyber security risks and financial inclusion. African Journal of Economic and Business Research, 4(2).

Opuni-Frimpong, J., Adefunso Dzorka, M., & Boadi, I. (2025). Governance's role in bank performance: cybersecurity committee assessment. Journal of Financial Reporting and Accounting, 23(2), 788-810.

Oyewole, A. T., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024). Cyber security risks in online banking: A detailed review and preventive strategies application. World Journal of Advanced Research and Reviews, 21(3), 625-643.

Wang, S., Asif, M., Shahzad, M. F., & Ashfaq, M. (2024). Data privacy and cyber security challenges in the digital transformation of the banking sector. Computers & security, 147, 104051.