



Cybersecurity Risks in Digital Banking and Their Effect on Financial Performance of Nigerian Commercial Banks

Jimoh Balogun 

Graduate School of Economics and Management, Ural Federal University Named after the First President of Russia B.N. Yeltsin (UrFU), Yekaterinburg, Russia
Email: balogunjimoh@yandex.com

How to cite this paper: Balogun, J. (2026) Cybersecurity Risks in Digital Banking and Their Effect on Financial Performance of Nigerian Commercial Banks. *Open Access Library Journal*, 13: e16056.
<https://doi.org/10.4236/oalib.1116056>

Received: September 20, 2026

Accepted: October 18, 2026

Published: October 21, 2026

Copyright © 2026 by author(s) and Open Access Library Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

Abstract

The rapid expansion of digital banking in sub-Saharan Africa has enlarged the attack surface available to cybercriminals targeting financial institutions. This study examines the nature, frequency and financial consequences of cybersecurity incidents at seven large Nigerian commercial banks over 2015-2023. It combines a documented-incident analysis, a pre/post comparison of bank performance and a fixed-effects panel regression. The regression indicates that a confirmed major cybersecurity incident is associated with a reduction in return on assets (ROA) of 0.547 percentage points ($p < 0.001$), and that larger confirmed losses are associated with lower ROA. For the six banks with an observable post-incident year, mean ROA fell from 2.00% to 1.47%, mean return on equity (ROE) from 14.75% to 10.65%, and the non-performing loan (NPL) ratio rose by 1.6 percentage points on average. The seven documented incidents generated aggregate direct losses of USD 32.5 million; ransomware, phishing/business email compromise (BEC) and mobile-channel (SIM-swap) fraud were the three costliest attack types, together accounting for 64% of that total. The estimates are interpreted as associations rather than causal effects. The paper discusses implications for the Central Bank of Nigeria (CBN) risk-based cybersecurity framework, international standards (ISO/IEC 27001, NIST CSF 2.0) and the operational-risk provisions of Basel III, and contributes to the literature on the microeconomic consequences of cybercrime in developing economies.

Subject Areas

Economics

Keywords

Cybersecurity Risk, Digital Banking, Financial Performance, Nigerian Commercial Banks, Panel Data Regression, ROA, ROE, CBN Cybersecurity Framework

1. Introduction

Driven by changing consumer behaviour, finance worldwide has moved heavily towards digital channels. Nigeria, one of Africa's largest economies by output, accelerated this shift after 2012, when the Central Bank of Nigeria (CBN) began rolling out its cashless-banking policy. According to the Nigeria Inter-Bank Settlement System (NIBSS), the value of instant payments processed in 2023 reached NGN 600 trillion, 55% above the NGN 387 trillion recorded in 2022 [1], while the number of transactions processed rose from about 5.1 billion to about 9.7 billion [2].

Digital growth is accompanied by growing exposure to cybercrime. NIBSS reported that banks had lost about NGN 9.5 billion to electronic fraud by August 2023, and the Financial Institutions Training Centre (FITC) found that the amount involved in fraud cases reported by banks rose by 277% between the first and second quarters of 2023, from NGN 2.58 billion to NGN 9.75 billion [3]. Globally, Cybersecurity Ventures projects that cybercrime could cost the world economy up to USD 10.5 trillion a year by 2025 [4].

Despite this exposure, research linking cyber incidents to the financial performance of Nigerian banks remains scattered and methodologically limited. Some sources catalogue fraud cases [5] [6], and others propose broad resilience models [7], but few connect incidents to profitability or stability indicators through statistical analysis. Much of the literature describes events without testing their financial impact.

This study addresses that gap through three objectives: 1) to document the types, frequency and direct financial losses of cybersecurity incidents at seven Nigerian commercial banks between 2015 and 2023; 2) to estimate the association between major incidents and bank performance, measured by ROA in the panel regression and by ROE and the NPL ratio in a descriptive pre/post comparison; and 3) to derive policy recommendations consistent with the CBN Risk-Based Cybersecurity Framework and Guidelines for deposit money banks and payment service providers [8].

Following the conceptual framework in Section 3.1, two hypotheses are examined. H1: A confirmed major cybersecurity incident is associated with lower ROA. H2: Conditional on an incident, larger confirmed losses are associated with lower ROA.

The paper is organised as follows. Section 2 reviews the theoretical foundations and prior studies. Section 3 describes the conceptual framework, data and meth-

odology. Section 4 presents the empirical findings. Section 5 sets out policy recommendations, and Section 6 concludes.

2. Theoretical Foundations and Literature Review

2.1. Theoretical Framework

Information asymmetry. Information asymmetry [9] was applied to information security by Anderson and Moore [10]. When attackers discover vulnerabilities before public disclosure, banks operate with incomplete knowledge of the risks they face, and defences lag behind threats. This imbalance can distort the pricing of risk and the allocation of capital [11], and efficiency declines as unobserved exposures accumulate, weakening financial outcomes. The link between concealed vulnerabilities and measured performance should therefore become observable over time.

Operational-risk regulation. Within the Basel operational-risk framework, cyber incidents are classified as external fraud or as business disruption and system failure events [12]. Under the standardised approach of the finalised Basel III reforms, historical loss data contribute to the calculation of operational-risk capital requirements [13]. This channel embeds cyber-related losses in performance indicators such as ROE by changing capital requirements and the way stability is measured across banks.

Resource-based view and signalling. Under the resource-based view [14] [15], adapted to information technology by Bharadwaj [16], security-related digital capabilities are strategic assets that sustain long-term competitive strength. Banks that underinvest in cybersecurity are expected to show more volatile operating results and greater reputational exposure. These expectations are consistent with signalling theory [17], under which investor trust responds to visible commitments to risk management.

2.2. Empirical Literature Review

Event studies of breach announcements provide the foundation of this literature. Cavusoglu, Mishra and Raghunathan [18] found a loss of about 2.1% in market value within two days of breach news, and later event studies, such as Goel and Shawky [19], likewise report negative market reactions to breach announcements. The direction of the evidence is consistent: adverse cyber incidents reduce firm valuation soon after they become known.

Research on banks in Africa and other developing economies is sparse. Nwankwo and Eze [20] analysed seven Nigerian financial institutions and found that electronic fraud was negatively correlated with ROA ($r = -0.61$). Using a fixed-effects model on 2016-2021 data, Yusuf, Sani and Balogun [21] found that each 10% rise in fraud costs reduced pre-tax profit by 3.2%. As far as the author can determine, neither study separates cyber-related breaches from general fraud, and neither accounts for differences in individual bank structure.

Internationally, Kamiya *et al.* [22] show that attacks involving the loss of per-

sonal financial information cause shareholder wealth losses much larger than the attacks' out-of-pocket costs, and that targets afterwards strengthen their risk management and information technology. At the sector level, the IMF [23] reports that financial firms have suffered direct cyber losses of almost USD 12 billion since 2004 and that the size of extreme losses has more than quadrupled since 2017, to USD 2.5 billion. The World Economic Forum ranks widespread cybercrime and cyber insecurity eighth among global risks by severity over both two- and ten-year horizons [24].

3. Conceptual Framework and Research Methodology

3.1. Conceptual Framework

Figure 1 presents the conceptual framework, grounded in the BCBS operational-risk taxonomy [12] and in the empirical approach of Cavusoglu *et al.* [18] and the IMF's analysis of cyber risk to financial stability [23]. Cybersecurity risk factors, which can be disaggregated by attack type following the MITRE ATT&CK® framework [25], are hypothesised to have a direct negative association with financial performance. Bank-level structural and regulatory variables are treated as control variables; no mediation or moderation is formally tested in this study. The empirical model reported in Section 4 uses the incident dummy and log loss as cyber-risk measures, four of the control variables, and ROA as the outcome; the remaining items in **Figure 1** are part of the conceptual framework only.

CYBERSECURITY RISK FACTORS	CONTROL VARIABLES	FINANCIAL PERFORMANCE OUTCOMES
▸ Phishing & social engineering ▸ Malware & ransomware ▸ DDoS attacks ▸ Insider threats ▸ Mobile banking fraud ▸ SIM-swap fraud ▸ API vulnerabilities In the model: CYBER (dummy) and LOG(LOSS)	▸ Bank size (total assets) ▸ Capital adequacy ratio ▸ Digital intensity index ▸ Loan-to-deposit ratio ▸ Regulatory compliance ▸ IT security investment	▸ Return on assets (ROA) ▸ Return on equity (ROE) ▸ Non-performing loans (NPL) ▸ Net interest margin (NIM) ▸ Customer deposit growth ▸ Operational cost ratio

Figure 1. Conceptual framework: cybersecurity risks and financial performance linkages.

Controls enter the ROA equation as regressors; the association of cyber risk with outcomes is estimated with bank and year fixed effects. Source: compiled by the author based on [12] [18] [23] [25].

3.2. Research Design and Data

Design. The variables are defined in **Table 1**. The study adopts a quantitative design combining three elements: a documented-incident analysis (**Table 2**), a descriptive comparison of bank performance in the years immediately before and after each incident (**Table 3**), and a fixed-effects panel regression of ROA (**Table 4**).

Sample and panel structure. The sample comprises seven large Nigerian com-

mercial banks (listed in **Table 2**), observed annually from 2015 to 2023 (nine years), giving a balanced panel of $7 \times 9 = 63$ bank-year observations. The banks were not randomly selected, so the results should not be generalised to the whole banking sector.

Data sources. Data are drawn from secondary sources: FITC quarterly summaries of fraud and forgery cases [3], CBN annual banking-supervision publications [6], NIBSS industry fraud reports [26], and the annual audited financial statements of each bank.

3.3. Model Specification and Inference

The baseline fixed-effects panel regression is specified as:

$$\text{ROA}_{it} = \alpha + \beta_1 \text{CYBER}_{it} + \beta_2 \text{LOG}(\text{LOSS})_{it} + \beta_3 \text{SIZE}_{it} + \beta_4 \text{CAR}_{it} + \beta_5 \text{DII}_{it} + \beta_6 \text{LDR}_{it} + \mu_i + \lambda_t + \varepsilon_{it}$$

where ROA_{it} is the return on assets of bank i in year t ; μ_i and λ_t are bank and year fixed effects; and ε_{it} is the idiosyncratic error. The other variables are defined in **Table 1**.

Table 1. Variable definitions.

Variable	Definition
ROA	Return on assets, %, from the banks' audited financial statements. Dependent variable in Table 4 .
ROE, NPL	Return on equity, %, and change in the non-performing loan ratio, percentage points. Used descriptively in Table 3 .
CYBER	Dummy equal to 1 if a confirmed major cybersecurity incident (Table 2) occurred at the bank in that year.
LOG (LOSS)	Natural logarithm of confirmed direct financial losses (Table 2).
SIZE	Natural logarithm of total assets.
CAR	Capital adequacy ratio, %.
DII	Digital Intensity Index: IT expenditure divided by total operating expenses.
LDR	Loan-to-deposit ratio, %.

A Hausman test [27] favours fixed over random effects ($\chi^2(6) = 18.74$, $p = 0.005$).

Inference. Standard errors follow Driscoll and Kraay [28], which are robust to heteroskedasticity, serial correlation and cross-sectional dependence. These estimators rely on large- T asymptotics, and with seven banks and nine annual periods their small-sample reliability is uncertain. The p -values in **Table 4** correspond to a normal reference distribution; with a t distribution with 8 degrees of freedom the p -value of the log-loss coefficient would be about 0.013 rather than 0.002, and that of the capital adequacy ratio about 0.047 rather than 0.021 (illustrative calculation). Results should therefore be read with caution, and a small-cluster robustness check (for example, a wild cluster bootstrap by bank) is a natural extension of this analysis.

Identification. The estimates are conditional associations. The design does not address reverse causality (for example, weaker banks may underinvest in security) or common economic shocks that affect both incident occurrence and profitability; year fixed effects absorb only shocks common to all banks. **Table 2** lists exactly one major incident per bank, so CYBER equals 1 in only seven bank-years (about 11% of the 63 observations). Because LOG(LOSS) can be non-zero only in incident years, CYBER and LOG(LOSS) are likely to be strongly correlated, which limits the precision with which their separate effects can be identified.

3.4. Threat Vector Classification

Attack labels follow the terminology of the MITRE ATT&CK® framework [25] and the CBN framework [8] where possible; some labels (BEC, ATM skimming, SIM swap) are industry terms that may not map one-to-one onto ATT&CK techniques. Where a label combines two vectors (for example Phishing/BEC), both are shown and the incident is counted once. Incidents are reported in **Table 2**.

4. Empirical Findings

4.1. Documented Cybersecurity Incidents in Nigerian Banks (2015-2023)

Table 2 lists the documented major incidents at the sampled banks, with the attack type and estimated direct loss. Figures are compiled from the secondary sources [3] [5] [6] [26].

Table 2. Major cybersecurity incidents in sampled Nigerian commercial banks (2015-2023).

Bank	Year	Attack type	Loss (USD m)	Share of total (%)	* Recovery period	Midpoint (months)*
First Bank Nigeria Plc	2017	Phishing/BEC	6.9	21.2	3 - 5 months	4.0
Zenith Bank Plc	2018	Malware/Insider threat	2.1	6.5	1 - 2 months	1.5
United Bank for Africa	2019	ATM skimming	4.3	13.2	2 - 3 months	2.5
Access Bank Plc	2020	Ransomware	8.7	26.8	4 - 6 months	5.0
Guaranty Trust Bank	2021	DDoS/data breach	3.5	10.8	2 - 4 months	3.0
Ecobank Nigeria	2022	Mobile fraud/SIM swap	5.2	16.0	2 - 3 months	2.5
Sterling Bank Plc	2023	API exploit/BEC	1.8	5.5	1 month	1.0
Total/mean			32.5	100.0		2.8

*Calculated from the table: share = loss ÷ 32.5; midpoint = middle of the reported recovery range. Sources: compiled by the author based on [3] [5] [6] [26].

The seven incidents total USD 32.5 million (mean USD 4.64 million; median USD 4.3 million), one per bank, with none recorded in 2015-2016. Ransomware was the costliest attack type (USD 8.7 million, 26.8% of the total), followed by phishing/BEC (USD 6.9 million, 21.2%) and mobile fraud/SIM swap (USD 5.2 million, 16.0%); together these three account for USD 20.8 million, or 64.0% of documented losses. The classification matters: BEC appears in two incidents (First

Bank Nigeria and Sterling Bank), and if aggregated, those losses total USD 8.7 million, equal to the ransomware loss.

Losses were not monotonic over time. They rose from USD 6.9 million in 2017 to a peak of USD 8.7 million in 2020 and then fell to USD 1.8 million in 2023, so **Table 2** does not show a steady increase in severity. The 2020 peak coincides with the pandemic-era acceleration of remote banking, but the data do not allow this link to be tested. Using the midpoints of the reported ranges, recovery took about 2.8 months on average (2.1 to 3.4 months using the lower and upper bounds). Longer recovery may have disrupted operations and customer trust, but this channel is not tested here.

4.2. Effect on Financial Performance Indicators

Table 3 compares performance in the year immediately before and the year immediately after each confirmed incident. Sterling Bank (incident in 2023) is not shown because the sample ends in 2023 and no post-incident year is available.

Table 3. Pre- and post-incident financial performance indicators, sampled Nigerian commercial banks.

Bank	ROA pre (%)	ROA post (%)	Δ ROA (pp)*	ROE pre (%)	ROE post (%)	Δ ROE (pp)*	Δ NPL (pp)
First Bank Nigeria	1.82	1.11	-0.71	12.4	7.8	-4.6	+1.9
Zenith Bank	2.31	1.95	-0.36	18.7	15.2	-3.5	+0.8
UBA	1.74	1.22	-0.52	14.1	9.4	-4.7	+2.1
Access Bank	1.56	0.93	-0.63	11.8	6.2	-5.6	+2.7
GTBank	3.12	2.74	-0.38	21.3	18.6	-2.7	+0.6
Ecobank Nigeria	1.45	0.88	-0.57	10.2	6.7	-3.5	+1.5
Mean	2.00	1.47	-0.53	14.75	10.65	-4.10	+1.60

*Post minus pre. “Mean” is the simple average of the six banks. Source: compiled by the author based on the banks’ audited financial statements and [6].

Mean ROA falls from 2.00% to 1.47% (-0.53 percentage points, about 26%) and mean ROE from 14.75% to 10.65% (-4.10 points, about 28%), while the NPL ratio rises by 1.6 points on average, which points to some deterioration in loan quality. The simple mean ROA decline is close to the regression coefficient in **Table 4** (-0.547). This comparison is descriptive: it uses one year on each side of the incident, has no control group, and does not remove common shocks such as the pandemic. The direction of the results is consistent with earlier international studies [22] [29].

Guaranty Trust Bank recorded the smallest ROE decline (2.7 percentage points). With one observation per bank, the data cannot show whether bank-specific security capabilities explain such differences, although the pattern is consistent with the view that stronger security capabilities soften financial impact [7] [16].

4.3. Panel Regression Results

Table 4 reports the fixed-effects regression of ROA with Driscoll-Kraay standard

errors [28].

Table 4. Fixed-effects panel regression: determinants of ROA in Nigerian commercial banks (2015-2023).

Variable	Coefficient (β)	Std. error	t-statistic	p-value
Constant	2.843	0.312	9.112	0.000***
Cybersecurity incident (dummy)	-0.547	0.104	-5.260	0.000***
Log (incident cost)	-0.213	0.067	-3.179	0.002***
Bank size (log assets)	0.184	0.055	3.345	0.001***
Capital adequacy ratio	0.096	0.041	2.341	0.021**
Digital Intensity Index	0.073	0.038	1.921	0.057*
Loan-to-deposit ratio	-0.038	0.029	-1.310	0.193
Fit statistics	R ² = 0.712 Adj. R ² = 0.689 F = 31.04*** N = 63			

Note: *p < 0.10; **p < 0.05; ***p < 0.01. Driscoll-Kraay standard errors; bank and year fixed effects. Dependent variable: ROA (%). Period: 2015-2023. Source: author's estimations.

The coefficient on the incident dummy (-0.547, p < 0.001) indicates that bank-years with a confirmed major incident are associated with ROA that is 0.547 percentage points lower, other things equal. This equals 27.4% of the mean pre-incident ROA of the six banks in Table 3 (2.00%). The coefficient on log incident cost (-0.213, p = 0.002) indicates that, conditional on an incident, larger losses are associated with a larger fall in ROA.

Consistency check. The total incident association is the sum of the dummy and loss terms, so it depends on the unit of LOSS. If LOSS is measured in USD million, the implied association ranges from -0.67 percentage points (USD 1.8 million) to -1.01 (USD 8.7 million), which exceeds the raw pre/post ROA declines of 0.36 to 0.71 points in Table 3. The difference may reflect year effects and controls, and should be interpreted with the caveats in Section 3.3.

Among the controls, bank size (0.184, p = 0.001) is positively associated with ROA, consistent with scale economies [16]; no interaction term is estimated, so this is a control association rather than a moderating effect. The capital adequacy ratio (0.096, p = 0.021) is also positively associated with ROA, consistent with the buffering role of capital against operational losses [12] [13]. The Digital Intensity Index (0.073, p = 0.057) is significant only at the 10% level; its sign is consistent with efficiency gains from IT investment, but the evidence is not conclusive. The loan-to-deposit ratio is statistically insignificant.

5. Policy Recommendations

Given that the evidence is associational, this paper offers the following recommendations at three levels of governance.

5.1. Regulatory and Supervisory Level (CBN/NDIC)

The CBN should require incident reports in a uniform format that includes quan-

tified monetary losses and feed them directly into its existing supervisory information systems. Rather than treating cyber breaches in isolation, supervision by the Nigeria Deposit Insurance Corporation (NDIC) could incorporate simulated cyber-loss assessments into annual examinations, guided by the BCBS principles [12] and the FSB Cyber Lexicon [30]. A further option is a dedicated, adjustable reserve for technology-related losses, analogous in design to the Basel III capital buffers [13] and calibrated to the national framework [8]. The CBN issued a revised framework for deposit money banks and payment service banks in 2024, effective 1 July 2024 [31], which postdates the sample; standardised loss reporting would let future studies assess its effects using supervisory data rather than secondary sources.

5.2. Institutional Level (Bank Management and Boards)

Boards should establish a Board Cybersecurity Committee separate from the Risk Management Committee, with quarterly reporting on key cybersecurity risk indicators (KCRIs), including mean time to detect (MTTD) and mean time to respond (MTTR), and should align their security management systems with recognised standards such as ISO/IEC 27001 [32] and the governance function of NIST CSF 2.0 [33]. Because bank size is positively associated with ROA (Table 4), consistent with scale economies, smaller Tier-2 banks could be encouraged to form shared security operations centre (SOC) consortia to lower per-unit security costs; this study does not test scale economies in cybersecurity directly. Chief Risk Officers should integrate cyber risk into economic-capital models using scenario-based stress testing [23].

5.3. National and International Coordination

The African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) entered into force on 8 June 2023, once the fifteenth ratification was deposited, nearly nine years after its adoption. Published status lists show that Nigeria signed the Convention in January 2024 but had not deposited ratification as of mid-2024 [34]. Further progress may depend less on declarations than on concrete national steps. Engagement with the UK National Cyber Security Centre (NCSC) could proceed alongside dialogue with the US Cybersecurity and Infrastructure Security Agency (CISA), and cross-border coordination would be strengthened by shared structures such as the FSB Cyber Lexicon [30]. The Federal Ministry of Finance, rather than a technology-focused agency, could coordinate these partnerships.

6. Conclusions

This study finds that major cybersecurity incidents at Nigerian commercial banks are associated with measurable deterioration in financial performance. A confirmed major incident is associated with ROA that is about 0.55 percentage points lower. The panel covers 2015-2023 and the seven documented incidents caused

direct losses of USD 32.5 million. These results are directionally consistent with international evidence [22] [23].

The findings suggest that cyber risk merits explicit treatment in capital planning and supervisory frameworks. The study does not permit a cost-benefit comparison between losses and security spending, because IT security investment is not measured. Bank size, capital adequacy and digital intensity are positively associated with ROA, but without interaction terms the results do not show that larger, better-capitalised or more digital banks recover faster from incidents.

Several limitations apply. First, the seven banks are large institutions that were not randomly selected, so the results may not generalise to smaller banks. Second, some incidents rely on self-reported disclosure, so the reported losses are probably lower bounds. Third, the CBN cybersecurity framework took effect on 1 January 2019 [8], the fifth of the nine sample years, so its effect cannot be isolated from other changes over the period. Fourth, with seven banks and seven incident observations, statistical power and the reliability of inference are limited, and the estimates cannot be interpreted causally.

Future research could extend the analysis to other African markets, use market-based measures such as Tobin's Q or credit default swap spreads, and exploit sudden policy changes to identify causal effects more credibly.

For Nigerian banks, cyber risk is a core financial and strategic risk rather than a peripheral operational concern, and it should be integrated into board-level decision-making.

Acknowledgements

The author gratefully acknowledges the scholarly mentorship of the academic staff of the Graduate School of Economics and Management, Ural Federal University named after the First President of Russia B.N. Yeltsin. This research was conducted in accordance with Ural Federal University Research Ethics Protocol No. GSEM-2024-07.

Conflicts of Interest

The author declares no conflicts of interest.

References

- [1] Nigeria Inter-Bank Settlement System (NIBSS) (2024) Nigeria Recorded N600 Trillion e-Payment Transactions in 2023. NIBSS.
<https://nibss-plc.com.ng/nigeria-recorded-n600-trillion-e-payment-transactions-in-2023/>
- [2] (2024) Amid Hitches, Nigeria's e-Payment Transactions Hit N600 Trillion. *The Guardian (Nigeria)*.
<https://www.pressreader.com/nigeria/the-guardian-nigeria/20240208/282132116347081>
- [3] Financial Institutions Training Centre (FITC) (2023) Reports of Fraud and Forgeries in Nigerian Banks (Quarter 2, 2023). FITC.

- [4] Cybersecurity Ventures (2023) Cybercrime to Cost the World \$10.5 Trillion Annually by 2025. <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>
- [5] Economic and Financial Crimes Commission (EFCC) (2022) Annual Report 2021. EFCC.
- [6] Central Bank of Nigeria (CBN) (2023) Annual Report on Banking Supervision 2022. CBN Publications.
- [7] Okunoye, A. and Karsten, H. (2022) Cybersecurity Resilience in African Financial Institutions: An Organisational Capability Perspective. *Information Systems Journal*, **32**, 298-327.
- [8] Central Bank of Nigeria (CBN) (2018) Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers. CBN. <https://www.cbn.gov.ng/out/2018/bsd/risk%20based%20cybersecurity%20framework%20final.pdf>
- [9] Akerlof, G.A. (1970) The Market for "Lemons": Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics*, **84**, 488-500. <https://doi.org/10.2307/1879431>
- [10] Anderson, R. and Moore, T. (2006) The Economics of Information Security. *Science*, **314**, 610-613. <https://doi.org/10.1126/science.1130992>
- [11] Stiglitz, J.E. and Weiss, A. (1981) Credit Rationing in Markets with Imperfect Information. *American Economic Review*, **71**, 393-410.
- [12] Basel Committee on Banking Supervision (BCBS) (2021) Revisions to the Principles for the Sound Management of Operational Risk. Bank for International Settlements.
- [13] Basel Committee on Banking Supervision (BCBS) (2017) Basel III: Finalising Post-Crisis Reforms. Bank for International Settlements. <https://www.bis.org/bcbs/publ/d424.htm>
- [14] Barney, J. (1991) Firm Resources and Sustained Competitive Advantage. *Journal of Management*, **17**, 99-120. <https://doi.org/10.1177/014920639101700108>
- [15] Wernerfelt, B. (1984) A Resource-Based View of the Firm. *Strategic Management Journal*, **5**, 171-180. <https://doi.org/10.1002/smj.4250050207>
- [16] Bharadwaj, A.S. (2000) A Resource-Based Perspective on Information Technology Capability and Firm Performance: An Empirical Investigation. *MIS Quarterly*, **24**, 169-196. <https://doi.org/10.2307/3250983>
- [17] Spence, M. (1973) Job Market Signaling. *The Quarterly Journal of Economics*, **87**, 355-374. <https://doi.org/10.2307/1882010>
- [18] Cavusoglu, H., Mishra, B. and Raghunathan, S. (2004) The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*, **9**, 70-104. <https://doi.org/10.1080/10864415.2004.11044320>
- [19] Goel, S. and Shawky, H.A. (2009) Estimating the Market Impact of Security Breach Announcements on Firm Values. *Information & Management*, **46**, 404-410. <https://doi.org/10.1016/j.im.2009.06.005>
- [20] Nwankwo, O. and Eze, G. (2021) Electronic Banking Fraud and Financial Performance of Deposit Money Banks in Nigeria. *International Journal of Economics and Financial Issues*, **11**, 34-44.
- [21] Yusuf, M.B., Sani, M.A. and Balogun, K. (2022) Cybersecurity Threats and Financial Performance: Evidence from Nigerian Deposit Money Banks. *Lapai International Journal of Management and Social Sciences*, **13**, 212-228.

- [22] Kamiya, S., Kang, J., Kim, J., Milidonis, A. and Stulz, R.M. (2021) Risk Management, Firm Reputation, and the Impact of Successful Cyberattacks on Target Firms. *Journal of Financial Economics*, **139**, 719-749. <https://doi.org/10.1016/j.jfineco.2019.05.019>
- [23] International Monetary Fund (IMF) (2024) Chapter 3. Cyber Risk: A Growing Concern for Macroeconomic Stability. In: *Global Financial Stability Report, April 2024*, IMF. <https://www.imf.org/-/media/Files/Publications/GFSR/2024/April/English/ch3.ashx>
- [24] World Economic Forum (WEF) (2023) The Global Risks Report 2023. 18th Edition, WEF. <https://www.weforum.org/reports/global-risks-report-2023/>
- [25] MITRE Corporation (2023) MITRE ATT&CK®. Version 14. <https://attack.mitre.org/>
- [26] Nigeria Inter-Bank Settlement System (NIBSS) (2023) Industry Electronic Fraud Report Q3 2023. NIBSS.
- [27] Hausman, J.A. (1978) Specification Tests in Econometrics. *Econometrica*, **46**, 1251-1271. <https://doi.org/10.2307/1913827>
- [28] Driscoll, J.C. and Kraay, A.C. (1998) Consistent Covariance Matrix Estimation with Spatially Dependent Panel Data. *Review of Economics and Statistics*, **80**, 549-560. <https://doi.org/10.1162/003465398557825>
- [29] Campbell, K., Gordon, L.A., Loeb, M.P. and Zhou, L. (2003) The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. *Journal of Computer Security*, **11**, 431-448. <https://doi.org/10.3233/jcs-2003-11308>
- [30] Financial Stability Board (FSB) (2018) Cyber Lexicon. FSB. <https://www.fsb.org/2018/11/fsb-publishes-cyber-lexicon/>
- [31] Central Bank of Nigeria (CBN) (2024) Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Banks. CBN.
- [32] ISO/IEC 27001:2022 (2022) Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements. International Organization for Standardization.
- [33] National Institute of Standards and Technology (NIST) (2024) The NIST Cybersecurity Framework 2.0. NIST.
- [34] African Union Commission (2024) Status of Ratification: African Union Convention on Cyber Security and Personal Data Protection. AU Commission. <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>