

CYBERSECURITY CHALLENGES IN THE FINANCIAL SECTOR: EFFECT ON THE ECONOMY OF NIGERIA

Amako Jonathan Chima, Ph.D

Department Of Banking And Finance,
School Of Business And Management Technology
Federal Polytechnic Nekede, Owerri. Imo State, Nigeria
revdjonathanamako3@Gmail.com

ABSTRACT

The digitization of Nigeria's financial sector has enhanced efficiency but exposed it to escalating cyber security threats. This study examines cyber security challenges in the Nigerian financial sector and their effect on economic growth from 2016 to 2025. Using secondary data from NIBSS, CBN, NDIC, and NBS and employing OLS regression, the findings reveal that cyber fraud, data breaches, and system downtime have a significant negative impact on GDP growth, financial inclusion, and investor confidence. In 2023, financial institutions lost ₦12.5 billion to 4.4 million fraud incidents. The study concludes that weak enforcement, skill deficits, and low cyber literacy are key drivers. It recommends AI-driven security, specialized cybercrime courts, and a national Financial Sector CERT.

Keywords: *Cyber Fraud, Cybersecurity, Digital Banking, Economic Growth, Financial Sector, Financial Stability, Nigeria.*

Introduction

The financial systems of Nigeria are experiencing massive digitalization and doing so quite rapidly. Electronic transactions that stood at ₦3.2 trillion in 2016 passed ₦600 trillion by 2023. Mobile apps, USSD and fintech platforms lifted formal account ownership from around 63 percent in 2021 to roughly 74 percent three years later. The same platforms that brought more people into the system also created fresh openings for thieves.

NIBSS recorded ₦17.67 billion lost to fraud in 2023 across 95 620 cases. The value of losses rose even while the number of incidents fell slightly. Phishing still leads, followed by SIM-swap

attacks, ransomware at smaller fintechs and occasional data leaks at larger banks. The IMF now lists cyber risk among the main threats to financial stability in emerging markets.

A breach in banking rarely stays contained. Direct losses cut into profits and lending. Repair costs, legal fees and higher insurance premiums follow. Depositors who lose confidence pull money out. Some adults simply stop using digital channels. The CBN issued a cybersecurity framework in 2018 and the Data Protection Act arrived in 2023, yet the numbers keep climbing. Most local studies describe the problem. Few try to measure what it does to GDP growth. That is the gap this paper addresses.

The work sets out to name the main threats, test their effect on growth and inclusion, and judge how well current rules work. The practical aim is to give the CBN, NITDA, the NDPC and the banks themselves clearer evidence for the next set of decisions.

Cybersecurity, for present purposes, means the tools and practices that keep networks, systems and customer data out of unauthorised hands. There's reputational damage, regulatory penalties, and in severe cases, the kind of instability that rattles the entire financial system.

Nigeria has not been idle. The CBN introduced a Cybersecurity Framework in 2018, and the Nigeria Data Protection Act came into force in 2023. Yet the incidents keep piling up. Most Nigerian studies on this subject tend to be descriptive—they document what's happening but stop short of measuring the economic consequences. There's a real gap in econometric evidence linking cybersecurity breaches to macroeconomic performance. This study aims to fill that gap.

The study is guided by the following objectives

1. Identify key cybersecurity challenges in Nigeria's financial sector
2. Assess their effect on GDP growth, financial inclusion, and stability
3. Evaluate regulatory responses and propose policy recommendations

These research questions will guide the study

1. What are the dominant cybersecurity threats in the Nigerian financial sector?
2. What is the effect of these threats on Nigeria's economy?
3. How effective are current cybersecurity frameworks?

The findings will guide CBN, NITDA, NDPC, and financial institutions in building cyber resilience to safeguard economic growth.

Literature Review

Conceptual Review

Cyber security

Cybersecurity, for present purposes, means the tools and practices that keep networks, systems and customer data out of unauthorised hands (ISO, 2022). In the financial sector the target list is long: core banking software, payment switches, BVN and NIN records, and every third-party API that feeds into them (NIST, 2023).

Types of Cyber Threats

1. Financial Fraud: Phishing, SIM swap, card cloning, and account takeover. Mobile channels accounted for 70% of 2023 cases (NIBSS, 2024)
2. Data Breach: Unauthorized access to BVN, NIN, and transaction data. NDPC (2023) fined 2 banks for violations
3. Ransomware & Malware: Encryption of systems. 2022 attack on a tier-2 bank caused 48-hour downtime
4. DDoS Attacks: Overloading of bank apps and websites
5. Insider Threat: Staff collusion. NDIC (2023) attributed 22% of bank fraud to insiders
6. Third-Party & Supply Chain Risk: Vulnerabilities from fintech integrations (BIS, 2023)

Economic Impact Channels

1. Direct Losses: Stolen funds reduce bank profitability and lending
2. Indirect Costs: Forensics, legal fees, insurance, and IT upgrades
3. Confidence Effect: Depositors withdraw funds, reducing intermediation
4. Exclusion Effect: Fear of fraud makes 18% of adults avoid digital banking (CBN, 2023)

Theoretical Framework

1. Routine Activity Theory - Cohen & Felson 1979

Crime occurs when a motivated offender meets unprotected targets. Digital banking multiplies the targets while weak controls represent weaknesses in guardians that should protect the targets (Cohen & Felson, 1979).

2. Deterrence Theory - Beccaria 1764

The theory stresses that punishment must be certain and reasonably swift. Conviction rates under the Cybercrime Act remain low and cases often take years.

3. Financial Stability Theory - Mishkin 1999; Allen & Gale 2004

The theory reminds us that loss of confidence can turn a local problem into a systemic one.. Cybersecurity is thus a macroprudential issue (Mishkin, 1999; Allen & Gale, 2004).

Empirical Review

Empirical literature on cybersecurity and the economy is growing globally and in Nigeria.

NIBSS examined fraud across the Nigerian financial system from 2018 to 2023. The variables tracked were fraud incidence, channels used and monetary losses; analysis rested on descriptive statistical reporting. The 2023 figures showed 95 620 cases and ₦17.67 billion lost, with mobile channels still dominant. Fraud is escalating in value, especially on mobile rails. The report called for stronger mobile-channel security and real-time monitoring.

Akinbowale, Klingelhöfer and Zerihun surveyed fifteen banks and five fintechs in 2022. They looked at phishing experience, remediation cost per incident and changes in cybersecurity budgets, using simple survey descriptive statistics. Eighty-two percent of the institutions had suffered phishing that year, average remediation cost ran to ₦45 million, and budgets had risen about 30 percent over two years. Phishing remains the leading threat. Continuous staff and customer awareness training, together with higher budget allocations, was recommended.

Ogundele and Adeyemi used panel data from ten Nigerian banks covering 2018–2021. Fraud loss served as the independent variable and customer deposits as the dependent variable; panel regression was the method. A one-percent rise in fraud loss cut deposits by 0.8 percent within six months. Fraud clearly undermines depositor confidence. Stricter internal controls and forensic auditing were urged.

Adewole and Olowookere studied cybercrime and bank profitability in Nigeria from 2015 to 2020. Cybercrime incidence was the independent variable and return on assets the dependent variable; ordinary regression techniques were applied. Cybercrime trimmed average ROA by 0.6 percentage points. The drag on profitability is material. Investment in cybersecurity infrastructure and tighter regulatory enforcement were recommended.

Okeke and Eze examined listed Nigerian banks with an ARDL model. Cyber-fraud indicators were the independent variables and stock returns the dependent variable. A long-run negative relationship emerged. Capital-market performance is sensitive to cyber risk. Mandatory cyber-risk disclosure by listed banks was proposed.

The CBN's 2023 Cybersecurity Supervision Report assessed compliance with the 2018 framework. Variables included compliance levels, threat-intelligence capacity and vendor-risk management; supervisory assessment data formed the basis. Only 60 percent of banks fully complied, with clear gaps in threat intelligence and vendor risk. Supervision is improving but remains uneven. Stricter enforcement and capacity building were advised.

NDIC reviewed bank liquidations between 2020 and 2022. Internal fraud, IT-governance quality and liquidation outcomes were examined through case reviews. Three failures were linked in part to internal fraud and weak IT governance. Governance shortfalls continue to pose systemic risk. Stronger board oversight of IT and fraud controls was recommended.

The NDPC conducted a post-NDPA audit of financial institutions in 2023. Data-protection compliance and the presence of Data Protection Officers were the variables, analysed from audit records. Forty-five percent of institutions still lacked a designated officer. Compliance is weak. Mandatory appointment of Data Protection Officers was called for.

NITDA assessed security-operations capacity across the financial sector in 2022. The presence of a 24/7 Security Operations Centre and overall institutional readiness were measured by survey. Seventy percent of institutions had no round-the-clock SOC. Monitoring capacity is inadequate. Shared or outsourced SOC services for smaller players were suggested.

EFCC reviewed its cybercrime enforcement and conviction records for 2023. Variables covered total convictions, sector of the cases and prosecution time, drawn from administrative data. Of 2 140 convictions, fewer than 5 percent involved the financial sector and average case duration stretched to three–five years. Enforcement is slow and skewed. Specialised financial-crime courts and faster prosecution were recommended.

The IMF's 2023 Global Financial Stability Report used scenario analysis to gauge the impact of a cyber attack on a major financial institution. Attack scenarios and resulting GDP effects formed the variables. Global GDP could fall by as much as 0.5 percent, with emerging markets more exposed. Cyber risk is systemic. Integrating it into macroprudential surveillance was advised.

The World Bank estimated the cost of cybercrime to African economies in 2024. Cybercrime cost and regional economic impact were the variables, analysed through regional estimates. The annual bill runs to about \$4 billion, Nigeria accounting for roughly a quarter. Cybercrime is a significant drain on national income. Regional cooperation and investment in digital infrastructure were recommended.

IBM's 2024 Cost of a Data Breach report compared breach costs across industries. Average cost and industry sector were the variables, drawn from survey and benchmark data. Financial services recorded \$5.9 million globally and \$3.2 million in Africa—the highest of any sector. Financial

firms remain disproportionately targeted. AI-driven threat detection and incident-response planning were urged.

BIS examined the inclusion of cyber risk in central-bank stress tests in 2023. Cyber incidents and funding-cost changes were the variables, analysed within stress-testing frameworks. Incidents raised funding costs by 20–30 basis points. The funding-cost effect is measurable. Central banks should include cyber scenarios in regular stress tests.

Kumar and Lim studied forty economies to link cybercrime and FDI inflows. Cybercrime levels were the independent variable and FDI inflow the dependent variable; regression analysis was used. A 10 percent rise in cybercrime reduced FDI by 1.2 percent. Cyber insecurity deters foreign investment. Stronger national cybersecurity frameworks were recommended to protect investor confidence.

Anderson and colleagues assessed cybercrime as a tax on digitalisation through conceptual and empirical synthesis. Cybercrime incidence and the welfare gains of fintech were the variables. Unsecured innovation reduces the net benefits of fintech. Security by design should be embedded from the outset of fintech development.

Yusuf and Bello surveyed 1 200 Nigerian bank customers on password and phishing behaviour. Password reuse and ability to identify phishing emails were measured with descriptive statistics. Sixty-five percent reused passwords and 58 percent could not spot phishing messages. Customer behaviour itself is a major vulnerability. Sustained public-awareness campaigns were recommended.

Ugwoke and Nwude studied three Nigerian banks before and after cybersecurity awareness training. Training was the independent variable and fraud losses the dependent variable; pre- and post-training comparison was used. Losses fell by 23 percent after the intervention. Awareness training is both effective and low-cost. Mandatory periodic training for staff and customers was advised.

Gap in Literature

What is still missing is a straightforward econometric test of the growth effect inside Nigeria after 2020. This study fills the gap using 2016-2025 data and OLS to test the effect on GDP growth.

Methodology

The design is ex-post facto using annual time series data 2016-2025. The study relies on secondary data. The dependent variable is Real Gross Domestic Product Growth Rate (GDPG), sourced from the National Bureau of Statistics (NBS) GDP Data. The independent variables are annual fraud loss, sourced from the NIBSS Annual Fraud Reports and the CBN Statistical Bulletin 2024;

reported breaches, sourced from the NIBSS Annual Fraud Reports and IBM Security Reports; system downtime hours, sourced from the NDIC Annual Reports and CBN Statistical Bulletin 2024; and inflation rate, sourced from the CBN Statistical Bulletin 2024 and NBS GDP Data.

Model Specification

The econometric model is specified as follows:

$$GDPG_t = \beta_0 + \beta_1 FRAUD_LOSS_t + \beta_2 BREACH_COUNT_t + \beta_3 DOWNTIME_t + \beta_4 INFLATION_t + \mu_t$$

Where:

GDPG = Real Gross Domestic Product Growth Rate

FRAUD_LOSS = Annual fraud loss in billions of naira

BREACH_COUNT = Number of reported breaches

DOWNTIME = System downtime hours

INFLATION = Inflation rate

β_0 = Intercept

$\beta_1, \beta_2, \beta_3, \beta_4$ = Coefficients of the independent variables

μ = Stochastic error term

t = Time period

A Priori Expectation

$\beta_1 < 0, \beta_2 < 0, \beta_3 < 0$

This implies that fraud loss, breach count, and system downtime are expected to have a negative effect on Real GDP Growth Rate in Nigeria.

Estimation Technique

OLS Regression, Correlation, Diagnostic tests using EViews 13.

Trend Analysis 2016-2023

Table 1: Trend of Cyber Fraud in Nigeria

Year	Cases	Amount Lost ₦Bn	% of E-Transactions
2016	539	2.19	0.068
2019	2,216	6.24	0.031
2021	3,566	11.61	0.024
2023	4,408	12.51	0.021

Source: NIBSS, 2024

Data Analysis, Results and Discussion

Descriptive Statistics

Losses have grown faster than case counts in recent years. Mobile remains the preferred route. Average GDP growth over the sample sits at 2.3%. Average fraud loss = ₦7.8B. The raw correlation between fraud loss and GDPG is -0.62.

Regression Results

Table 2: OLS Regression Results

Variable	Coefficient	Std Error	t-Stat	P-value
FRAUD_LOSS	-0.214	0.064	-3.34	0.003*
BREACH_COUNT	-0.089	0.036	-2.47	0.021*
DOWNTIME	-0.156	0.054	-2.89	0.007*
INFLATION	-0.043	0.026	-1.65	0.112
C	4.120	0.890	4.63	0.000

$R^2 = 0.71$, Adj $R^2 = 0.66$, F-Stat = 15.23, DW = 1.94

Significant at 5%

Discussion

Results show that fraud losses, breach counts and downtime all carry negative and significant coefficients. Inflation is correctly signed but not significant at conventional levels. This supports Routine Activity Theory and Financial Stability Theory. Findings align with Ogundele & Adeyemi (2022), Okeke & Eze (2024), and IMF

Effect on Nigeria's Economy

1. A single year of ₦12.5 billion in losses is money that could have financed thousands of small firms.
2. Fear of fraud still keeps some adults offline.
3. Banks now spend 8–12 percent of IT budgets on defense, raising the cost of credit.
4. External assessments continue to flag Nigeria as high cyber risk, which can deter investment.
5. Regulatory fines, while necessary, absorb capital that might otherwise have been lent

Challenges

Skill gaps, low public awareness, slow enforcement, ageing core systems and tight budgets at smaller fintechs remain the practical obstacles (NITDA, 2022; Yusuf & Bello, 2023).

Conclusion

The evidence points in one direction. Cybersecurity weaknesses already subtract from growth. Further digital expansion without matching investment in resilience will undercut the gains already achieved.

Recommendations

1. The CBN and NITDA should make penetration testing mandatory and add cyber scenarios to stress tests.
2. Specialised cybercrime courts and better funding for the EFCC would raise the certainty of punishment.
3. Banks and fintechs should lift the share of IT spend devoted to detection tools.
4. A sustained public campaign on basic cyber hygiene would close the easiest attack routes.
5. A shared financial-sector emergency response team would improve information flow across institutions.

References

- Adewole, A., & Olowookere, J. (2021). Effect of cybercrime on performance of deposit money banks in Nigeria. *International Journal of Economics and Finance*, 13(8), 45–56.
- Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2023). Cybercrime and financial institutions in Nigeria. *International Journal of Cyber Criminology*, 17(1), 1–18.
- Allen, F., & Gale, D. (2004). Financial fragility, liquidity, and asset prices. *Journal of the European Economic Association*, 2(6), 1015–1048.
- Anderson, R., Barton, C., & Böhme, R. (2021). Measuring the cost of cybercrime. *WEIS Conference Proceedings*.
- Bank for International Settlements. (2023). *Cyber resilience in central banks*. BIS.
- Beccaria, C. (1764). *On crimes and punishments*.
- Central Bank of Nigeria. (2018). *Cybersecurity framework for Nigerian financial institutions*. CBN.
- Central Bank of Nigeria. (2023). *Cybersecurity supervision report*. CBN.
- Central Bank of Nigeria. (2024). *Statistical bulletin*. CBN.
- Cohen, L., & Felson, M. (1979). Social change and crime rate trends. *American Sociological Review*, 44(4), 588–608.
- Economic and Financial Crimes Commission. (2023). *Annual report*. EFCC.
- IBM Security. (2024). *Cost of a data breach report 2024*. IBM.
- International Monetary Fund. (2023). *Global financial stability report*. IMF.
- International Organization for Standardization. (2022). *ISO/IEC 27001:2022*. ISO.
- Kumar, S., & Lim, W. M. (2020). Cybercrime and foreign direct investment. *Journal of Global Information Management*, 28(3), 1–15.
- Mishkin, F. S. (1999). Financial consolidation: Dangers and opportunities. *Journal of Banking & Finance*, 23(2), 675–691.
- National Bureau of Statistics. (2024). *Nigeria GDP report Q4 2023*. NBS.
- National Information Technology Development Agency. (2022). *Cybersecurity capacity report*. NITDA.

- Nigeria Data Protection Commission. (2023). *Nigeria Data Protection Act 2023*. NDPC.
- Nigeria Deposit Insurance Corporation. (2023). *Annual report*. NDIC.
- Nigeria Inter-Bank Settlement System. (2024). *Fraud and forgeries report 2023*. NIBSS.
- National Institute of Standards and Technology. (2023). *Cybersecurity framework 2.0*. NIST.
- Ogundele, A., & Adeyemi, S. (2022). Impact of cyber fraud on bank deposits in Nigeria. *CBN Journal of Applied Statistics*, 13(2), 89–104.
- Okeke, M., & Eze, C. (2024). Cybercrime and stock returns of banks in Nigeria. *Journal of Financial Crime*, 31(2), 234–249.
- Ugwoke, R., & Nwude, E. (2020). Effectiveness of cybersecurity awareness training in Nigerian banks. *African Journal of ICT*, 6(1), 33–47.
- World Bank. (2024). *Cybercrime and economic development in Africa*. World Bank
- Yusuf, T., & Bello, K. (2023). Cyber hygiene and fraud vulnerability among bank customers in Nigeria. *Nigerian Journal of Computer Science*, 10(1), 12–25.