International Journal of Business & Law Research 14(2):165-176, April-June, 2026

© SEAHI PUBLICATIONS, 2026 www.seahipublications.org ISSN: 2360-8986

doi:10.5281/zenodo.19559881

Cybersecurity Threats and Sustainable Growth of Listed Deposit Money Banks in Nigeria

Omaliko Emeka Leonard (Ph.D)

Department of Accountancy,
Faculty of Management Sciences,
Nnamdi Azikiwe University, Awka, Nigeria

ABSTRACT

This study empirically investigated the relationship between cybersecurity threats and sustainable growth of listed deposit money banks in Nigeria. Thus, two hypotheses were formulated to guide the investigation and the statistical test of parameter estimates was conducted using least squares regression model operated with E-Views.12. Survey design was adopted and the data for the study was obtained through the use of e-questionnaire survey sent to the various Staff WhatsApp Group Platform of the selected listed deposit money banks operative in Awka, Anambra State Nigeria. The results of the study therefore revealed that there is significant and positive association between cybersecurity threats and sustainable growth of listed deposit money banks in Nigeria at 1% level of significance. Based on this, the study concludes that sustainable growth of deposit money banks in Nigeria is largely affected by cybersecurity threats. In lieu of the findings of the study, the study recommends that to reduce the adverse effect of cyberattack threats on sustainable growth of banks, management of listed deposit money banks in Nigeria must focus on strengthening their cybersecurity frameworks. This entails deploying advanced security solutions and proactive risk management practices to curb financial losses from cyber incidents, thereby protecting financial performance and supporting long-term sustainability.

Keyword: Cybersecurity; Cyberattack; Threats; Sustainable Growth

1. INTRODUCTION

Nigeria's banking sector has undergone a remarkable digital transformation over the past decade, with the rapid expansion of mobile banking, instant payment platforms, and open banking initiatives. This digital expansion has significantly enhanced financial inclusion, improved transaction efficiency, and expanded the customer base of deposit money banks (Ohiani, 2021). However, the same digital channels that have enabled this growth have also exposed the financial system to an escalating wave of cybersecurity threats, creating a critical tension between innovation and security that threatens the sustainable growth of listed deposit money banks in Nigeria.

The magnitude of the cybersecurity challenge confronting Nigerian banks is staggering. According to Check Point Software Technologies' 2024 African Perspectives on Cyber Security Report, the Nigerian banking and financial sector recorded an average of 4,718 cyberattacks per week, which is 182.01 percent higher than the global average of 1,673 weekly attacks (BusinessDay, 2024; Check Point Software Technologies, 2024). This alarming frequency underscores the sector's heightened vulnerability and the aggressive targeting of Nigerian financial institutions by both domestic and international cybercriminals and further illustrating the relentless nature of the threat environment.

The financial consequences of these attacks have been catastrophic. Data from the Nigeria Inter-Bank Settlement System (NIBSS) revealed that the banking sector lost ₦52.26 billion to fraud in 2024,

representing a sharp 195 percent increase from the ₦17.67 billion recorded in 2023. This trajectory of escalating losses is further confirmed by the Financial Institutions Training Centre (FITC), whose Fraud and Forgery Report indicated that Nigerian banks lost ₦53.4 billion to cybercriminals in just the first nine months of 2024, a staggering 468 percent surge from the ₦9.4 billion lost during the same period in 2023 (Adepetun, 2024). Thus, the situation has continued to deteriorate and persistent threat of fraud continues to erode the financial health and operational stability of banks.

According to Olukoyede (2025), cybersecurity breaches impose substantial non-financial costs that threaten the sustainable growth of listed deposit money banks. Reputational damage, erosion of customer trust, and increased regulatory scrutiny are inevitable consequences of major security incidents. The FITC also warned that the increasing rate of fraud is eroding the trust in the financial system, with customers becoming increasingly apprehensive about the safety of their deposits (Adepetun, 2024). This trust deficit is particularly problematic for listed banks, whose market valuation depends not only on current profitability but also on investor confidence in their long-term viability and governance structures. Furthermore, cybersecurity threats have been shown to adversely impact financial inclusion a key driver of banking sector growth in Nigeria as potential customers, particularly those in underserved rural areas, may resist adopting digital banking channels due to security concerns. Research has also established a strong correlation between cybercrime and business performance in the Nigerian banking industry, indicating that cybersecurity vulnerabilities directly undermine the financial and operational metrics that underpin sustainable growth (Nwankwo, 2023; Udoinyang, 2024).

Despite the gravity of the cybersecurity challenge, existing research on the Nigerian banking sector has largely focused on isolated aspects of the problem. Studies have examined the relationship between technology innovation and bank competitiveness (Ohiani, 2021), the impact of cybersecurity on microfinance bank sustainability (Nwankwo, 2023), and the correlation between online banking adoption and cybercrime growth (Udoinyang, 2024). However, there is a notable dearth of comprehensive empirical research specifically examining how cybersecurity threats affect the sustainable growth of listed deposit money banks in Nigeria. The existing literature has not adequately addressed how cyber threats influence the multidimensional sustainability metrics of listed deposit money banks including financial performance, market valuation, customer retention, regulatory compliance costs, and long-term strategic resilience. Furthermore, while studies have established that a 10 percent increase in online banking adoption is associated with a 3.42 percent increase in cybercrime (Udoinyang, 2024), the implications of this relationship for the sustainable growth trajectory of listed deposit money banks remain underexplored.

This study therefore seeks to address these critical gaps by systematically investigating the relationship between cybersecurity threats and the sustainable growth of listed deposit money banks in Nigeria. Specifically, the research aims to:

1. Examine the effect of ransomware cyberattack on sustainable growth of listed deposit money banks in Nigeria.
2. Evaluate the effect of phishing cyberattack on sustainable growth of listed deposit money banks in Nigeria.

By addressing these objectives, the study will contribute to both academic knowledge and practical policy formulation, providing evidence-based insights for bank executives, regulators, and policymakers seeking to safeguard the sustainable growth of Nigeria's banking sector in an increasingly hostile digital environment.

2. Review of Related Literature

2.1. Cybersecurity Threats

Cybersecurity as defined by National Institute of Standards and Technology (2012) is a foundational definition used in many cybersecurity frameworks and is valued for its comprehensive scope. It encompasses the potential for harm to a wide range of entities, including national interests, making it suitable for high-level strategic risk assessments.

According to Jeyaraj and Zadeh (2022), cybersecurity threat is rooted in the academic literature and emphasizes the potential for disruption to core information security principles confidentiality, integrity, and availability. It frames a threat as a likelihood and an attempt, distinguishing it from a vulnerability or a successful attack. It is specific to the banking sector, emphasizing the deliberate attempt to exploit vulnerabilities and the dual motivation of personal gain and operational disruption (Udoinyang, 2024).

Cybersecurity is the threat of financial losses, disruption and/or reputational damage from a malicious breach of an entity's information systems. It is the possibility of or attempt of gaining unauthorized access to a device or system or network using a data communication pathway (Darem et al., 2023).

2.1.1 Phishing Cyberattack

It is a technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person. The study went further to note that phishing is an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques (Destiny, 2025).

According to Federal Deposit Insurance Corporation (2026), phishing cyberattack is the use of seemingly legitimate e-mail messages and Internet Web sites to deceive consumers into disclosing sensitive information, such as bank account information, Social Security numbers, credit card numbers, passwords, and personal identification numbers (PINs).

2.1.2 Ransomware Cyberattack

Ransomware is a type of malware that attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid. It is a type of malware identified by specified data or systems being held captive by attackers until a form of payment or ransom is provided (Financial Crimes Enforcement Network, 2020).

According to NIST (2021), ransomware is a form of malicious software (malware) designed to block access to a computer system or data, often by encrypting data or programs on information technology (IT) systems to extort ransom payments from victims in exchange for decrypting the information and restoring victims' access to their systems or data. It is a form of malicious software that infiltrates computer systems or networks and uses tools like encryption to deny access or hold data hostage until the victim pays a ransom, usually in Bitcoin.

2.1.3 Contributory Factors to Cybersecurity Threats in Nigeria

Several factors contribute to cyberthreats vulnerability in Nigeria. It includes but not limited to:

i. **Inadequate Technical Safeguards:** Many Nigerian entities function without modern security infrastructure such as network monitoring systems, perimeter defenses, or data encryption rendering them defenseless against cyber intrusions (Isaac, 2025).
ii. **Deficient Public Awareness:** A considerable majority of Nigerian citizens lack fundamental knowledge of cybersecurity hygiene, significantly increasing their risk of falling victim to phishing and psychological manipulation tactics (Saidu et al., 2022).
iii. **Enforcement Deficits in Regulation:** Despite the legal framework provided by statutes like the 2015 Cybercrimes Act, practical application of the law is hindered by institutional resource gaps and systemic graft (Ayotunde, 2025).
iv. **Expanded Digital Exposure:** The dramatic growth in mobile connectivity and online participation across Nigeria has inadvertently broadened the landscape of exploitable targets for cyber adversaries (Willie, 2025).
v. **Vulnerabilities from New Tech Adoption:** The accelerated deployment of AI, cloud computing services, and IoT ecosystems has outpaced security planning, exposing enterprises to a wave of new, unmitigated threats (Kunle et al., 2017).

2.1.4 The Role of Central Bank of Nigeria (CBN) in Shaping Cybersecurity Threats in Nigeria

According to Ama et al. (2024), the Central Bank of Nigeria occupies a pivotal position in cultivating cybersecurity resilience within the financial services industry and intercepts in curbing cyberattacks through the following;

i. **Issuance of Regulations and Directives:** The CBN crafts and imposes compliance standards, including the Risk-Based Cybersecurity Framework and Guidelines tailored for banks and payment service operators.
ii. **Performing Threat Evaluations:** It systematically appraises the cyber vulnerabilities inherent within financial institutions and delivers advisory on robust risk containment.
iii. **Implementation of Cybersecurity Levies:** The bank enforces a statutory cybersecurity charge on digital payments to generate funding for sector-wide security initiatives.
iv. **Monitoring Adherence:** It supervises the financial sector to verify strict conformance with established cybersecurity policies and procedural requirements.
v. **Provision of Operational Guidance:** The CBN furnishes technical assistance and strategic counsel to help organizations elevate their overall security posture.
vi. **Collaboration:** CBN partners with complementary oversight bodies to foster a unified and efficient regulatory environment.
vii. **Championing Security Consciousness:** The CBN actively drives educational outreach programs aimed at bolstering cybersecurity vigilance among both professional entities and the general populace.

2.1.5 Sustainable Growth.

Tutun and Som (2019) define sustainable growth as expansion that can be maintained profitably to generate future value. The notion of sustainable growth gained prominence through Higgins's influential 1977 work, which introduced the sustainable growth rate model as a means of articulating the operational boundaries within which a firm can realistically expand. Consequently, the sustainable growth rate serves as an indicator of whether a company's sales trajectory aligns with its internal capabilities and the prevailing conditions of the financial marketplace. Omaliko and Okpala (2022) assert that corporate sustainable growth encompasses both financial performance metrics and non-financial disclosures related to social and environmental initiatives, which collectively enable firms to pursue expansion in a manner that is both enduring and socially responsible.

The study of Buffa et al. (2020) submitted that to ensure sustainable growth, organizations must concede the following:

i. Accountability for the social, environmental, and economic footprint of the organization.
ii. Transparency regarding all decisions and operations that influence stated responsibilities.
iii. Responsiveness to the concerns and interests of stakeholders.
iv. Strict and universal adherence to the rule of law.

2.2 Theoretical Framework

The theoretical framework which gives the meaning of a word in terms of the theories on cybersecurity threats and sustainable growth established in this study is Fraud Diamond Theory

2.2.1 Fraud Diamond Theory

The Fraud Diamond Theory, initially advanced by Wolfe and Hermanson (2004), provides a comprehensive analytical framework for understanding the relationship between cybersecurity threats and the sustainable growth of deposit money banks in Nigeria. This theory posits that fraudulent activities, including cyber-enabled financial crimes, materialize only when four distinct elements converge: pressure, opportunity, rationalization, and capability. When applied to the contemporary digital banking environment, this framework illuminates how cybersecurity vulnerabilities are not merely technological shortcomings but are deeply rooted in human behavior, organizational culture, and institutional governance all of which exert a direct and measurable influence on a bank's capacity for long-term sustainable expansion.

The first element, pressure, refers to the motivational drivers that compel individuals to contemplate or execute fraudulent cyber activities. Within the banking context, pressure manifests in various forms, including financial distress experienced by under-compensated employees, the imposition of unrealistic performance targets by management, or the relentless pursuit of illicit profits by organized cybercriminal syndicates targeting the financial system (Wolfe & Hermanson, 2004). When internal stakeholders face

unmanageable personal or professional pressures, they become increasingly susceptible to the overtures of external hackers seeking insider collaboration. Similarly, external threat actors are motivated by the immense financial rewards associated with breaching the digital vaults of commercial banks. The manifestation of this pressure translates directly into financial losses that erode the capital base of the bank, thereby depleting the very resources required to fund expansion, technological upgrades, and shareholder returns all essential components of sustainable growth.

The second element, opportunity, represents the structural and procedural gaps within a bank's operational environment that allow a cyber threat to be executed successfully. In the era of rapid digital transformation characterized by mobile banking, instant payments, and open banking application programming interfaces, the attack surface of Nigerian deposit money banks has expanded exponentially, thereby creating a proliferation of opportunities for malicious actors (Firdaus et al., 2022). Opportunity encompasses weak authentication protocols, unpatched software vulnerabilities, inadequate segregation of duties within the information technology department, and insufficient monitoring of transaction logs. When a bank fails to implement robust cybersecurity controls, it essentially leaves the door ajar for exploitation. The relationship between opportunity and sustainable growth is inverse and direct: banks that operate with porous security perimeters incur recurring financial losses, face heightened regulatory penalties, and suffer reputational damage that increases their cost of capital, all of which severely constrains their ability to achieve and maintain sustainable growth trajectories.

The third element, rationalization, addresses the psychological mechanism by which perpetrators justify their unethical or criminal actions to themselves. Wolfe and Hermanson (2004) noted that most fraudsters do not view themselves as criminals; rather, they construct cognitive narratives that neutralize the moral weight of their actions. In the context of cybersecurity threats within banks, an employee with privileged system access might rationalize the theft of funds or the sale of customer data by convincing themselves that the bank is highly profitable and "can afford the loss," or that they are merely "borrowing" the money with the intention of repayment. External hackers, meanwhile, may rationalize their attacks by viewing the bank as an impersonal, faceless corporate entity rather than an institution comprising individual depositors and stakeholders. This element is particularly insidious because it bridges the gap between a technical vulnerability (opportunity) and the decision to act. A weak ethical culture within a bank, or a governance environment perceived as unfair, can significantly lower the psychological barriers to committing cyber fraud. Consequently, this internal decay undermines the trust and integrity that are foundational to sustainable growth, as investors and customers alike lose confidence in the bank's ability to safeguard assets.

The fourth and distinguishing element of the model is capability. Wolfe and Hermanson (2004) introduced this element to the existing fraud triangle, arguing that while pressure, opportunity, and rationalization may exist, fraud cannot occur on a significant scale unless the perpetrator possesses the requisite skills, position, and psychological fortitude to execute and conceal the act. In the realm of cybersecurity threats, capability is paramount. It refers not only to the technical acumen required to deploy ransomware, orchestrate phishing campaigns, or bypass encryption protocols but also to the positional authority that enables an insider to override security alerts or authorize fraudulent wire transfers without detection. Recent empirical research underscores the primacy of capability in the banking sector. For instance, a study conducted on the Ghanaian banking industry revealed that while pressure and opportunity are pervasive, the specific capabilities of management or information technology personnel are often the decisive factor in whether a fraud scheme materializes (Firdaus et al., 2022). Furthermore, investigations into the Nigerian financial landscape have repeatedly highlighted the role of insider-backed cyberattacks, wherein technically capable bank employees collude with external hacking syndicates to siphon billions of naira from customer accounts. This convergence of internal access and external technical skill exemplifies the capability element of the fraud diamond in action. The implication for sustainable growth is severe: a bank staffed by capable but ethically compromised individuals operates in a perpetual state of existential risk, where even the most sophisticated technological defenses can be rendered obsolete by human treachery.

Therefore, Fraud Diamond Theory clarifies that cybersecurity threats are not random, exogenous shocks to the banking system; rather, they are endogenous consequences of human behavior and organizational conditions. The presence of pressure motivates the act, opportunity provides the access point, rationalization justifies the morality of the act, and capability ensures its successful execution. The interplay of these four elements directly compromises the financial performance, operational resilience, and reputational capital of listed deposit money banks in Nigeria. As financial losses from cyber fraud escalate and erode earnings per share, and as investor trust diminishes in the face of recurring breaches, the foundational pillars of sustainable growth; profitability, stability, and stakeholder confidence are systematically weakened. Therefore, any strategic initiative aimed at fostering sustainable growth in the Nigerian banking sector must address not only the technological dimensions of cybersecurity but also the human and behavioral dimensions elucidated by the Fraud Diamond framework. Thus, the study was anchored on Fraud Diamond Theory

2.3 Empirical Review

Destiny (2025) investigated the evolving landscape of cybersecurity vulnerabilities within Nigeria's financial sector, focusing on emerging threat patterns and their implications for banking institutions. The study employed a mixed-methods approach, combining quantitative analysis of documented cyber incidents with qualitative insights obtained from industry practitioners. The study used a multi-faceted strategy for enhancing cybersecurity resilience, emphasizing the critical importance of robust technological infrastructure, comprehensive workforce training, and enhanced inter-institutional collaboration. The findings revealed a marked escalation in cyberattacks, with ransomware, phishing campaigns, and insider threats identified as the predominant concerns confronting the industry. The study enriches the growing body of literature on cybersecurity in emerging economies and delivers practical policy recommendations for Nigerian regulators and financial entities.

Adejoke and Adeniran (2025) investigated the impact of cybersecurity threats on the financial performance of listed commercial banks in Nigeria, with a specific focus on determining the degree to which financial losses attributable to cyber threats influence earnings per share. An ex-post facto research design was employed for the investigation. The target population consisted of all fourteen commercial banks listed on the Nigerian Exchange Limited, from which a sample of ten banks was purposively selected using judgmental sampling. Secondary data were sourced from the audited annual financial statements of the sampled banks, as well as from annual reports published by the Nigeria Deposit Insurance Corporation and fraud reports issued by the Nigeria Inter-Bank Settlement System covering the period from 2012 to 2023. Data analysis incorporated descriptive statistics, including measures of central tendency and dispersion, while hypothesis testing was performed using robust least squares regression. The findings revealed that financial losses resulting from cybersecurity threats exert a negative effect on the earnings per share of listed commercial banks in Nigeria. The study concludes that cybersecurity threats transcend mere technical or operational difficulties; they constitute significant financial vulnerabilities that exert a direct and measurable impact on banks profitability.

Ama et al. (2024) conducted an investigation into the cybersecurity challenges confronting deposit money banks in Nigeria, with particular attention to the proactive strategies employed by both financial institutions and their customers to mitigate these threats. The study adopted a descriptive research design and utilized a census sampling approach, wherein data were gathered from the staff of the selected deposit money banks through the administration of structured questionnaires. Statistical analysis was performed using the Statistical Package for the Social Sciences (SPSS). The findings revealed that the principal cybersecurity challenges facing the banking sector included pharming attacks, identity theft, SIM swap fraud, skimming and website cloning, as well as smishing and vishing schemes. The study further identified key contributory factors, notably deficiencies within the banks' internal control frameworks, insider misconduct perpetrated by bank employees, and a pervasive lack of security awareness and ignorance among the banking public. In response to these threats, banks were found to have implemented various countermeasures, including data encryption protocols, mandatory periodic password changes, and the filtering or blocking of unsolicited electronic communications. The study concluded by offering

recommendations for the regular updating of security infrastructure, routine evaluation of internal control systems, and the execution of comprehensive customer education initiatives.

Fatoki (2023) investigated the influence of cybersecurity on the prevalence of financial fraud within Nigerian banks, addressing multiple dimensions including the classification of electronic fraud types, the underlying drivers of cyber fraud, the obstacles hindering its prevention, the consequential effects on banking institutions, and potential remedial strategies. The study employed a survey methodology targeting employees drawn from six Nigerian banks, with a sample comprising 557 staff members identified through a multistage sampling procedure. Data were gathered via a structured questionnaire and subsequently analyzed using the Statistical Package for the Social Sciences (SPSS). The findings indicated that prevalent forms of cyber fraud within the banking sector include computer viruses, hacking incidents, phishing attacks, pharming schemes, and employee-perpetrated internal fraud. Contributory factors to the incidence of cybercrime were found to encompass inadequate supervisory oversight, commercial pressures associated with performance target attainment, collusion between internal staff and external actors, deficient data encryption protocols, and the engagement of third-party service providers. Furthermore, the study identified several impediments to effective cyber fraud prevention, notably the absence of unified national standards, insufficient technological infrastructure, inherent internet vulnerabilities, and low levels of customer awareness regarding security risks.

Rufus et al. (2022) explored the role of cybersecurity in fostering financial innovation among deposit money banks in Nigeria. The study emphasized that the country's rapid population expansion, combined with the persistent issue of financial exclusion, has rendered the pursuit of financial innovation a critical imperative for the banking sector. Employing a survey research design, the data for the study was collected through the use of structured questionnaire administered to a purposively selected sample of 56 senior staff members from key functional departments. The participating banks represented 93% of total market capitalization as of December 31, 2021. Analysis of the data, conducted using both descriptive and inferential statistical methods, revealed that cybersecurity operationalized through risk management and bank monitoring exerted a statistically significant and positive influence on the financial innovation activities of Nigerian deposit money banks.

Ogunwale (2020) investigated the impact of cybercrime on the operational performance of deposit money banks in Nigeria through a theoretical review approach. The study concluded that the diligent enforcement of relevant cybersecurity regulatory frameworks would not only mitigate the incidence of cybercrime but also strengthen public confidence in the banking sector.

3. METHODOLOGY

The study adopted a survey design in order to examine the relationship between cybersecurity threats and sustainable growth in Nigeria using some selected listed deposit money banks in Awka, Anambra State as a reference point. The selected banks include; GTB Plc, Fidelity Bank Plc, UBA Plc, First Bank Plc, FCMB Plc, Access Bank Plc and Zenith Bank Plc. Data for the study was collected through the use of e-questionnaire survey sent to the various Staff WhatsApp Group Platform of the selected banks in Awka Anambra State Nigeria out of which 54 responses were received and recorded. The recorded responses were therefore used in the data analysis. The e-questionnaire survey was designed where respondents were asked to assess the relationship between cybersecurity threats and sustainable growth of listed deposit money banks in Nigeria using Likert five point scales referred as: (1) To a Very High Extent (THE), (2) To a High Extent (HE), (3) Neutral (N), (4) To a Very Low Extent (TLE) and (5) To a Low Extent (LE).

The collected data was transformed to scale measurement using Likert five point scale and the hypotheses were statistically tested using Least Squares Regression Model with the aid of E-Views 12.

3.1 Model Specification

In line with the previous studies, the present study designed a model in examining the relationship between cybersecurity threats and sustainable growth in Nigeria. The functional model for the study is shown below as thus:

SG = F (RCA, PCA)

The explicit form of regression designed for the study is shown below as thus:
$SG = \beta_0 + \beta_1 RCA + \beta_2 PCA + \varepsilon$
Where:
SG = Sustainable Growth
RCA = Ransomware Cyberattack
PCA = Phishing Cyberattack
μ = Stochastic Term
β_1- β_2= Coefficient of Regression Equation
β_0 = Constant coefficient (intercept) of the model
'*A Priori*' is given as: $\beta_0, \beta_1, \beta_2 > 0$
Decision Rule: accept Ho if P-value >1-5% significant level otherwise reject Ho

4. DATA ANALYSIS AND RESULTS

4.1 Distribution of Respondents Responses

The distribution of the respondents' responses was exposited on table 4.1.1 below as thus:

Table 4.1.1: Analysis of the Respondents Responses

	Item	Respondents	Percentage
	Listed Deposit Money Banks		
1.	GTB Plc	9	17
2.	Fidelity Bank Plc	6	11
3.	UBA Plc	7	13
4.	First Bank Plc	8	15
5.	FCMB	5	9
6.	Access Bank Plc	9	17
7.	Zenith Bank Plc	10	18
	Total	**54**	**100.00**

Source: Field Survey (2025)

Table 4.1.1 above shows that 9 respondents representing 17% of the respondents were the staff of GTB Plc; 6 respondents representing 11% of the respondents were the staff of Fidelity Bank Plc, 7 respondents representing 13% of the respondents were the staff of UBA Plc, 8 respondents representing 15% of the respondents were the staff of First Bank Plc, 5 respondents representing 9% of the respondents were the staff of FCMB Plc, 9 respondents representing 17% of the respondents were the staff of Access Bank Plc while the remaining 10 respondents representing 18% of the respondents were the staff of Zenith Bank Plc

4.2: Descriptive Summary

Table 4.2.1: Descriptive Statistics

	SG	RCA	PCA
Mean	4.510000	4.380000	4.090000
Median	4.020000	4.080000	3.880000
Maximum	4.830000	4.640000	4.190000
Minimum	4.140000	4.110000	3.220000
Std. Dev.	0.198762	0.209784	0.119873
Skewness	0.287642	1.898973	2.255541
Kurtosis	2.000822	1.000827	1.898733
Jarque-Bera	0.127676	0.339843	0.568431
Probability	0.567252	0.890982	0.254763
Sum	20.12544	118.2653	72.67263
Sum Sq. Dev.	37.56353	98.09873	28.09833
Observations	5	5	5

Source: E-View 12 Computational Results (2026)

From Table 4.2.1 above, the mean (average), maximum values, minimum values, standard deviation and Jarque-Bera Statistics (Normality Test) were shown. It was found that sustainable growth has a positive value of 4.51 which implies that sustainable growth of listed deposit money banks in Nigeria is determined by the magnitude of cybersecurity threats faced. The distribution is platykurtic since the kurtosis (2.00) is less than 3, implying that the outliers are few. The Jarque-Bera probability of 0.57 is greater than 0.05, which means that the distribution of sustainable growth comes from a normal distribution.

The average value of ransomware cyberattack (RCA) for the sampled banks was 4.38 with a standard deviation value of 0.21. This means that ransomware cyberattack is a determinant of sustainable growth of listed deposit money banks in Nigeria. The maximum value of RCA was 4.64 and the minimum value of RCA was 4.11 reflects a narrow range suggesting that the sampled banks experienced ransomware cyberattack. The distribution for the study is platykurtic since the kurtosis (1.00) is less than 3, implying that the outliers are few. However, the Jarque-Bera probability of 0.89 is greater than 0.05, which means that the distribution of ransomware cyberattack is not different from a normal distribution.

The mean value of phishing cyberattack (PCA) for the sampled banks was 4.09 with a standard deviation value of 0.12. This means that sustainable growth of listed deposit money banks in Nigeria is largely affected by phishing cyberattack. The maximum value of PCA was 4.19 and the minimum value of PCA was 3.22 suggests that the sampled banks experience phishing cyberattack. The distribution for the study is platykurtic since the kurtosis (1.89) is less than 3, implying that the outliers are few. However, the Jarque-Bera probability of 0.25 is greater than 0.05, which means that the distribution of phishing cyberattack comes from a normal distribution.

4.3: Test of Hypotheses

Least Squares was developed to test the linear relationship between the dependent and independent variables. It was operated using E-Views 12 as shown in the table 4.3.1 below:

Table 4.3.1: Result on the Relationship between Cybersecurity Threats and Sustainable Growth of Listed Deposit Money Banks in Nigeria

Dependent Variable: SG
Method: Least Squares
Date: 04/9/26 Time: 05:53
Sample: 1-5
Included observations: 5

Variable	Coefficient	Std. Error	t-Statistic	Prob.
RCA	0.989367	0.109833	9.007921	0.0000
PCA	0.589873	0.089763	6.571449	0.0000
C	1.908733	0.177633	10.74537	0.0000

R-squared	0.879272	Mean dependent var	5.167353
Adjusted R-squared	0.836441	S.D. dependent var	2.676637
S.E. of regression	0.777353	Akaike info criterion	9.887633
Sum squared resid	4.098773	Schwarz criterion	8.234452
Log likelihood	11.654341	Hannan-Quinn criter.	9.537656
F-statistic	9.765263	Durbin-Watson stat	2.176338
Prob(F-statistic)	0.000000		

Source: Author's Computation (2026)

4.4: DISCUSSION OF FINDINGS

The coefficient of determination R^2 shows 0.88 indicating that the overall model explained 88 percent of the total variations in the dependent variable (sustainable growth). Thus implies that the independent variable (cybersecurity threats) can only explain 88 percent of change in SG of listed deposit money banks in Nigeria leaving 12 percent unexplained. This is to say that there are other factors that could affect sustainable growth of listed deposit money banks in Nigeria other than cybersecurity threats. The sig. (or p-value) is .0001 which is below the .01 level; hence, we conclude that the overall model is statistically significant, or that the variables have a significant and joint effect on the dependent variable. With this, the researcher affirms the validity of the regression model adopted in this study.

The results of the regression are therefore slated below as follows:

H_{01}: Ransomware cyberattack has no significant effect on sustainable growth of listed deposit money banks in Nigeria. This hypothesis was tested and the result of this regression as exposited on table 4.3.1 indicates that the relationship between RCA and SG is positive and significant. This is justified with the P-value (significance) of 0.0000 which is less than the 1% level of significance adopted. Likewise the result of positive coefficient of 0.989 indicates that sustainable growth of listed deposit money banks in Nigeria is largely affected by ransomware cyberattack. We consequently rejected null the hypothesis and accepted the alternate hypotheses which contends that ransomware cyberattack has significant effect on sustainable growth of listed deposit money banks in Nigeria. This aligns with the a priori expectations of Destiny (2025), Adejoke and Adeniran (2025) who found positive and significant association between cybersecurity attacks and financial performance of listed deposit money banks in Nigeria.

H_{02}: Phishing cyberattack has no significant effect on sustainable growth of listed deposit money banks in Nigeria. This hypothesis was tested and the result of this regression as exposited on table 4.3.1 indicates that the relationship between PCA and SG is positive and significant. This is justified with the P-value (significance) of 0.0000 which is less than the 1% level of significance adopted. Likewise the result of positive coefficient of 0.589 indicates that sustainable growth of listed deposit money banks in Nigeria is largely determined by the magnitude of phishing cyberattack. We consequently rejected the null hypothesis and accepted the alternate hypotheses which portends that phishing cyberattack has significant effect on sustainable growth of listed deposit money banks in Nigeria. This is in tandem with the results of Ama et al. (2024), Fatoki (2023) who found that cybersecurity attacks affect financial performance of listed deposit money banks in Nigeria.

5. CONCLUSION

The study examined the relationship between cybersecurity threats and sustainable growth of listed deposit money banks in Nigeria. In achieving this, the study employed a survey research design, and data was collected through e-questionnaire. The results of the study showed a positive and significant association between cybersecurity threats and sustainable growth of listed deposit money banks in Nigeria. Hence, the study concludes that cybersecurity threats affect/hinder the sustainable growth of listed deposit money banks in Nigeria.

5.1 RECOMMENDATION

The study recommends as follows;

1. To reduce the adverse effect of ransomware threats on the sustainable growth of banks, management of listed deposit money banks in Nigeria must focus on strengthening their cybersecurity frameworks. This entails deploying advanced security solutions and proactive risk management practices to curb financial losses from cyber incidents, thereby protecting financial performance and supporting long-term sustainability.
2. Banks should implement proactive systems for detecting and reporting phishing attacks. Regular cybersecurity audits, along with the deployment of real-time response mechanisms, can help lessen the harmful effects of phishing incidents on the sustainable growth of banks.

REFERENCES

Adejoke, A., & Adeniran, C. (2025). Cybersecurity Threats and Financial Performance of Listed Commercial Banks in Nigeria. *Asian Journal of Advanced Research and Reports 19*(4), 381-94. https://doi.org/10.9734/ajarr/2025/v19i4990.

Adepetun, A. (2024). Banks lose N53.4b to frauds in 9 months as attacks rise by 65%. *The Guardian*. https://guardian.ng/business-services/banks-lose-n53-4b-to-frauds-in-9-months-as-attacks-rise-by-65/[reference:20]

Ama, G.A.N., Onwubiko, C.O. and Nwankwo, H.A. (2024). Cybersecurity challenge in Nigeria deposit money banks. *Journal of Information Security, 15*, 494-523. https://doi.org/10.4236/jis.2024.154028

Ayotunde, J. (2025). The effectiveness of cybercrime investigations and prosecution in Nigeria. February.

Buffa, F., Franch, M., & Rizio, D. (2022). Environmental management practices for sustainable business models in small and medium sized hotel enterprises. *Journal of Cleaner Production, 19*(4), 656-664

BusinessDay. (2024, November 21). Nigerian banks face 182% more weekly attacks than global counterparts. *BusinessDay*. https://businessday.ng/news/article/nigerian-banks-face-182-more-weekly-attacks-than-global-counterparts/[reference:22]

Check Point Software Technologies. (2024). *2024 African perspectives on cyber security report*. Check Point Software Technologies.

Darem, A. A., Alhashmi, A., Alkhaldi, T., Alashjaee, A., Alanazi, S., & Ebad, S. (2023). Cyber threats classifications and countermeasures in banking and financial sector, *IEEE Access*, *11*, 125138-125158. doi: 10.1109/ACCESS.2023.3327016.

Destiny, Y. (2025). Analysis of emerging cybersecurity threats in Nigeria's financial sector: trends, impacts, and mitigation strategies. *International Journal of Research and Innovation in Social Science, 9*(7), 1094-1103

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.

Federal Deposit Insurance Corporation. (2026). *Guidance on safeguarding customers against e-mail and internet-related fraudulent schemes* (FIL-27-2004). https://www.fdic.gov/news/financial-institution-letters/2004/fil2704a.html

Financial Crimes Enforcement Network. (2020). *Advisory on ransomware and the use of the financial system to facilitate ransom payments* (FIN-2020-A006). U.S. Department of the Treasury. https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf

Firdaus, R., Xue, Y., Gang, L., & Sibt e Ali, M. (2022). Artificial intelligence and human psychology in online transaction fraud. *Frontiers in Psychology*, 13, Article 947234. https://doi.org/10.3389/fpsyg.2022.947234

Isaac, O. (2025). Evaluating cybersecurity risks in Nigeria's commercial banking sector: An empirical analysis. February.

Jeyaraj, A., & Zadeh, A. H. (2022). Exploration and exploitation in organizational cybersecurity. *Journal of Computer Information Systems*. Advance online publication. Taylor & Francis.

Kunle, O. J., Olubunmi, O. A., & Sani, S. (2017). Internet of things prospect in Nigeria: Challenges and solutions. *2017 IEEE 3rd International Conference on Electro-Technology for National Development, NIGERCON 2017, (November),* 736–745. https://doi.org/10.1109/NIGERCON.2017.8281942

National Institute of Standards and Technology. (2012). *NIST Special Publication 800-30 Revision 1: Guide for Conducting Risk Assessments.* U.S. Department of Commerce.

National Institute of Standards and Technology. (2021). *NIST special publication 800-53 revision 5: Security and privacy controls for information systems and organizations*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5

Nwankwo, C. (2023). Effect of cyber security on business sustainability of listed microfinance banks in Nigeria. *Rajagiri Management Journal*, 17(2), 145-162. https://doi.org/10.1108/RAMJ-2023-0012[reference:31]

Ogunwale, H. (2020). The impact of cybercrime on Nigeria's commercial banking system." *International Journal of management and Business Studies, 2*(3), 75-78.

Ohiani, A. S. (2021). Technology innovation in the Nigerian banking system: Prospects and challenges. *Journal of Financial Services Marketing*, 26(2), 112-128. https://doi.org/10.1057/s41264-020-00088-2[reference:32]

Olukoyede, O. (2025, May 28). EFCC raises alarm over insider-backed cyberattacks on Nigerian banks. *Ripples Nigeria*. https://www.ripplesnigeria.com/efcc-raises-alarm-over-insider-backed-cyberattacks-on-nigerian-banks/[reference:33]

Omaliko, E., & Okpala, E. (2022). Tax aggressiveness and sustainability of listed oil and gas firms in Nigeria: Does firm size matter? *International Journal of Economics and Business Management, 8*(2), 48-60. https://doi.org/10.56201/ijebm.v8.no2.2022.pg48.60

Rufus, A., Olubunmi, O., Modupe, A., Abimbola, A. (2022). Cyber security and financial innovation of selected deposit money banks in Nigeria. *Universal Journal of Accounting and Finance, 10*(3), 643-652. DOI: 10.13189/ujaf.2022.100302.

Saidu, I. R., Musa, M. N., & Abdulkadir, A. S. (2022). Social Engineering Risk and Its Effect on Nigeria's Electronic Banking Security. *NDA Journal of Military Science and Disciplinary Studies*, *1*(2), 1–14.

Tutun, M & Som, S. (2019). Intellectual capital and corporate sustainability growth: The Indian evidence", *Journal of Business, Economics and Environmental Studies*, *9*(2), 5-15

Udoinyang, N. (2024, October 3). The relationship between cybercrime and the Nigerian economy: Causes, implications and the path forward. *European Conference on Security and International Studies*. https://ecsis.org/publications/cybercrime-nigerian-economy[reference:36]

Willie, A. (2025). Cybercrime and its Impact on Nigeria's Digital Economy. February.

Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal, 74*(12), 38–42.