***Original Research Article***

**Cybersecurity Threats and Financial Performance of Listed Commercial Banks in Nigeria**

# Abstract

The study examined the effect of cybersecurity threat on financial performance of listed commercial banks in Nigeria. The study specifically examined the extent to which financial loss from cybersecurity threat affects the earnings per share of listed commercial banks in Nigeria. This study adopted an ex-post facto research design. The population of the study comprises all fourteen (14) listed commercial banks on the Nigerian Exchange Limited. From this population, a sample of ten (10) listed commercial banks were selected using judgmental sampling technique. Data for the study were obtained from secondary sources, particularly the audited annual financial statements of the sampled banks, Nigeria Deposit Insurance Corporation annual reports and Nigeria Inter-Bank Settlement System fraud reports from 2012 to 2023. In addition to the descriptive analysis of the data using measures of central tendency and measures of dispersion, hypothesis testing was conducted using robust least square regression. The study found that financial losses from cybersecurity threats have a negative effect on the earnings per share of listed commercial banks in Nigeria (β = -0.013024, p = 0.0000). In conclusion, cybersecurity risks are not just technical or operational challenges but also crucial financial concerns that directly affect the bottom line. The study recommends that the management of listed commercial banks in Nigeria prioritize investment in robust cybersecurity frameworks by implementing advanced security measures and proactive risk management strategies to minimize financial losses resulting from cyber incidents, safeguarding the bank's financial performance.

*Key words:* Cybersecurity Threat, Financial Performance, Earnings Per Share

# 1.0 Introduction

In recent years, the global financial ecosystem has undergone a significant transformation driven by rapid technological advancements, increased digitalization, and growing internet penetration. As businesses across sectors increasingly adopt digital channels to improve efficiency and customer engagement, financial institutions, particularly commercial banks have emerged as major players in the digital economy (Nwankwo, Kanyangale, Anoke & Eze, 2023). In Nigeria, the banking sector has embraced a wide range of digital technologies such as online banking, mobile applications, cashless transactions, and automated teller machines (ATMs), all aimed at improving service delivery and broadening financial inclusion. This digital transformation has contributed significantly to the competitiveness and growth of the banking industry in the country. However, alongside these benefits comes a heightened exposure to cybersecurity threats (Ama, Onwubiko & Nwankwo, 2024; Kshetri, 2023; Jang-Jaccard & Nepal, 2022). The convergence of finance and technology, while advantageous, presents new challenges in the form of cyberattacks, data breaches, ransomware, phishing, and other forms of cybercrimes that threaten the integrity, confidentiality, and availability of financial services. The worst of them all seems to be the financial losses due to cybersecurity threats of which last five year data are presented below in Figure 1.

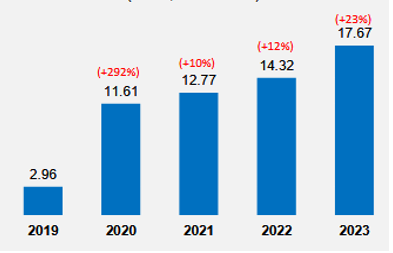


Figure 1 Amount Lost to Cyberfraud in the last five years (in billions of naira)

Source: Nigeria Inter-Bank Settlement System. (2024)

The Nigerian banking system, as part of a globally interconnected digital network, is increasingly vulnerable to the risks posed by malicious cyber actors (Anaege, Eneh, Inweregbu & Okwuego, 2025). Despite regulatory efforts by institutions such as the Central Bank of Nigeria (CBN) to enforce cybersecurity frameworks, the sector has witnessed a surge in cybercrime activities. In 2020 alone, Nigerian financial institutions reported hundreds of attempted cyberattacks, which led to a total cyber loss of N11.61 billion with its attendant reputational losses (Nigeria Inter-Bank Settlement System, 2024). The growing sophistication of cybercriminals, combined with existing infrastructural and regulatory challenges, means that banks must remain vigilant in protecting sensitive customer data and ensuring operational continuity (Ogunwale, 2020). These developments place cybersecurity at the center of strategic and operational priorities for commercial banks in Nigeria (Fatoki, 2023).

In today's digital business environment, effective cybersecurity is no longer a luxury or a reactive tool—it is a strategic imperative (Austin-Olowo, Anike & Ailemen, 2023). The proliferation of data-driven technologies, artificial intelligence, and interconnected devices has made businesses more susceptible to cyberattacks. For commercial banks, whose operations rely heavily on the trust and confidence of customers, robust cybersecurity measures are critical. An effective cybersecurity system protects digital assets, ensures regulatory compliance, and sustains customer trust by preventing unauthorized access to sensitive information (Fatoki, 2023). In an era marked by increasing data breaches and identity theft, the failure to invest adequately in cybersecurity could result in dire consequences not only for the individual institution but for the financial system as a whole (Samoei & Gatobu, 2024). As customer expectations grow and regulatory demands become more stringent, financial institutions must adopt proactive cybersecurity strategies that encompass technical, organizational, and human dimensions.

Moreover, as financial services expand their digital footprint, cyber risk management is fast becoming a key performance indicator. Banks must balance the dual objective of promoting innovation and ensuring security. Cybersecurity, therefore, plays an instrumental role in protecting assets, sustaining financial stability, and maintaining the overall resilience of financial institutions (Ama, Onwubiko & Nwankwo, 2024; Bose & Leung, 2024). In Nigeria, where infrastructural and digital literacy gaps exist, the need for effective cybersecurity becomes even more pronounced. The ability of a bank to guard against cyber threats often serves as a benchmark for operational excellence and long-term sustainability (Ogunwale, 2020). Thus, institutions that prioritize cybersecurity are more likely to foster customer loyalty, attract investment, and gain competitive advantage in a digitally driven marketplace.

Furthermore, the increasing cost of implementing cybersecurity frameworks, employee training, technological upgrades, and incident response mechanisms also affect the financial bottom line of commercial banks. While these costs are often necessary to prevent larger financial losses, they do place additional pressure on operational budgets. In response to the rising threats, the Central Bank of Nigeria has issued various guidelines, such as the Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers, to help institutions bolster their cyber defenses. There is a growing consensus among stakeholders that cybersecurity must be integrated into the broader risk management and governance structures of banks, rather than treated as a purely technical issue. However, in spite of the rapid adoption of digital banking channels and the increasing volume of electronic transactions, many listed commercial banks in Nigeria continue to face significant vulnerabilities to cyber threats (Ama, Onwubiko & Nwankwo, 2024). Reports of cyberattacks such as phishing, malware infiltration, denial-of-service (DoS) attacks, and financial fraud have become more frequent, often leading to service disruptions, unauthorized access to customer data, and financial losses (Samoei & Gatobu, 2024). Moreover, the implementation of cybersecurity policies remains inconsistent across banks, with gaps in technological investment, employee training, incident response capacity, and compliance with regulatory guidelines issued by the Central Bank of Nigeria. These challenges expose banks to persistent cyber risks and compromise their ability to maintain financial stability in an increasingly volatile digital landscape.

Financially, banks suffer direct monetary losses, increased operational costs, and reduced profitability due to fraud, system downtimes, and recovery expenses (Ogunwale, 2020). Reputationally, frequent breaches erode customer trust, result in client attrition, and affect market perception particularly for listed banks whose performance is closely monitored by investors and regulators. There is also the risk of sanctions and penalties from non-compliance with cybersecurity regulations. These issues collectively undermine the financial performance of affected banks, making it difficult for them to sustain growth, attract investment, and remain competitive in the digital economy. As cyber threats continue to evolve in scale and sophistication, the lack of robust cybersecurity frameworks poses a significant threat to the financial health and resilience of Nigeria’s commercial banking sector (Anaege, Eneh, Inweregbu & Okwuego, 2025). This reality highlights the need for an empirical examination of how cybersecurity threats impact the financial performance of listed commercial banks in Nigeria.

# 1.1 Objectives of the Study

The main aim of the study is to examine the effect of cybersecurity threat on financial performance of listed commercial banks in Nigeria. However, the study specifically examines the extent to which financial loss from cybersecurity threat affects the earnings per share of listed commercial banks in Nigeria.

# 1.2 Hypothesis

H01: Financial losses from cybersecurity threat do not significantly affect the earnings per share of listed commercial banks in Nigeria.

# 2.0 Literature Review

# 2.1 Conceptual Review

# 2.1.1 Cybersecurity Threat

A cybersecurity threat refers to any potential malicious act or activity that seeks to compromise the confidentiality, integrity, or availability of digital systems, networks, and data (Ama, Onwubiko & Nwankwo, 2024). It encompasses a wide range of intentional actions or unintended events that exploit vulnerabilities in information technology infrastructures, aiming to disrupt operations, gain unauthorized access to sensitive information, or cause damage to systems and data. In essence, a cybersecurity threat represents the possibility of harm or attack originating from digital or online sources, whether human-driven or automated, that can negatively impact the security of information systems (Anaege, Eneh, Inweregbu & Okwuego, 2025).

The term "cybersecurity threat" is inherently associated with risk and vulnerability in the digital landscape (Nwankwo, Kanyangale, Anoke & Eze, 2023). It does not imply actual harm but rather the existence of a credible possibility that such harm could occur if defenses are breached. Cybersecurity threats can stem from external factors such as hackers, cybercriminals, terrorist organizations, and state-sponsored entities, as well as from internal sources like disgruntled employees or negligent staff (Ama, Onwubiko & Nwankwo, 2024). These threats are dynamic and continually evolve, reflecting changes in technology, attacker sophistication, and systemic weaknesses in organizational cybersecurity measures.

Importantly, cybersecurity threats are not limited to attacks that result in immediate data theft or financial fraud (Austin-Olowo, Anike & Ailemen, 2023). They also include actions that may cause long-term damage, such as undermining system integrity, planting malware for future exploitation, or disrupting critical operations through denial-of-service attacks (Aminu, 2024). As businesses and governments increasingly rely on digital technologies to deliver services, the scope of cybersecurity threats has expanded to include threats against national infrastructure, corporate systems, individual privacy, and even societal stability (Samoei & Gatobu, 2024). Understanding cybersecurity threats involves recognizing them as latent dangers in the digital environment, dangers that if realized, can have far-reaching consequences for economic, operational, and reputational stability across sectors.

# 2.1.2 Financial Performance

Financial performance refers to the measure of how well a business or organization utilizes its assets, resources, and operational strategies to generate income, create shareholder value, and achieve financial sustainability over a specific period (Ayuba, Bambale, Ibrahim & Sulaiman, 2019). It serves as an indicator of a company’s overall financial health, efficiency, and profitability, and is typically assessed using financial statements, accounting ratios, and performance metrics (Nworie, Moedu & Onyali, 2023). Financial performance reflects both short-term outcomes and long-term financial strength, offering stakeholders hints on how effectively the company is being managed.

Financial performance embodies the results of financial decisions made by management in areas such as investment, financing, and operational execution. It is a comprehensive concept that evaluates whether a firm is making profits (Aminu, 2024) as well as the quality of those profits. Financial performance provides a benchmark for comparing companies within an industry and guides investor confidence, regulatory assessments, and managerial decisions. High financial performance is often associated with efficient cost control (Aggreh, Abiahu & Nworie, 2023), strategic investment, risk management (Nwafor & Nworie, 2025), and customer retention, while poor financial performance may signal inefficiencies, declining market share, or strategic missteps (Raveendra, Singh, Singh & Kumar, 2018).

Importantly, financial performance is not confined to accounting numbers alone; it encompasses how well a firm aligns its financial goals with its operational realities (Gartenberg, Prat & Serafeim, 2019). In the context of commercial banks, financial performance reflects how efficiently the institution manages its interest income, loan portfolios, non-performing assets, and operational expenses to generate value for shareholders. It also includes the bank's ability to withstand economic shocks, regulatory changes, and competitive pressures. Thus, financial performance is a multidimensional measure that integrates profitability, liquidity, solvency, and market valuation to provide a holistic picture of organizational success and financial soundness.

# 2.1.3 Earnings Per Share (EPS)

Earnings per share (EPS) is a financial metric that represents the portion of a company's net profit allocated to each outstanding share of common stock (Nworie, Moedu & Onyali, 2023). It is calculated by dividing the net earnings available to common shareholders by the average number of outstanding shares during a specific financial period. EPS serves as a key indicator of a company’s profitability and is widely used by investors, analysts, and stakeholders to assess the financial performance of a firm, especially in relation to shareholder value (Arsal, 2021). It translates a company’s total profit into a per-share basis, thereby enabling comparisons across firms and industries.

EPS is significant because it provides a direct linkage between a company’s profitability and the return that shareholders can expect to receive from their investment. A higher EPS typically indicates a more profitable company, which may lead to higher dividend payments or reinvestment into the business for growth (Kumar, 2017). It reflects the efficiency with which a company converts its earnings into value for its shareholders, and it plays a vital role in influencing investor sentiment and stock price movements in the capital market. Publicly traded companies often report basic and diluted EPS in their financial statements, with the latter accounting for potential dilution from convertible securities or stock options.

# 2.2 Theoretical Framework

The Fraud Diamond Theory was proposed by David Wolfe and Dana Hermanson in 2004 as an enhancement of the widely recognized Fraud Triangle Theory developed by Donald Cressey (Hermanson & Wolfe, 2024). While the Fraud Triangle focused on three elements—pressure, opportunity, and rationalization—Wolfe and Hermanson introduced a fourth dimension: capability. They argued that fraud cannot occur unless the individual has not only the motivation and opportunity but also the skills, position, and traits necessary to commit and conceal the fraud. The addition of capability makes the Fraud Diamond a more comprehensive tool in understanding and detecting fraudulent behavior in organizations (Mansor & Abdullahi, 2015).

The main postulation of the Fraud Diamond Theory is that four elements must be present for a fraud to occur: pressure (a need or incentive to commit fraud), opportunity (a situation that enables fraud to be carried out), rationalization (the mindset that justifies the fraud), and capability (the ability of the person to recognize the opportunity and exploit it) (Mansor, 2015). The theory emphasizes that even if the first three conditions exist, fraud is unlikely without a person who has the competence, confidence, and authority to exploit the system. Capability, therefore, is the critical factor that differentiates between people who merely contemplate fraud and those who actually commit it (Mansor & Abdullahi, 2015).

This theory is highly relevant to the topic “Effect of Cybersecurity Threat on Financial Performance of Listed Commercial Banks in Nigeria.” Cybersecurity threats often involve intentional acts of fraud carried out by individuals with both opportunity and capability including insiders or skilled external attackers. When banks have weak cybersecurity systems, they create opportunities for such individuals to exploit vulnerabilities, resulting in financial losses, data breaches, and reputational damage. The Fraud Diamond Theory provides a useful lens to understand how various human and systemic factors combine to make banks susceptible to cyber threats, which in turn affect their financial performance. The theory supports the argument that strengthening cybersecurity reduces both opportunity and capability for fraud, thereby protecting the financial health of banks.

# 2.3 Empirical Review

Anaege, Eneh, Inweregbu, and Okwuego (2025) explored the impact of cybersecurity threats on the operational efficiency and regulatory compliance of microfinance banks (MFBs) in Anambra State, Nigeria, with a focus on MFBs using the National Association of Microfinance Banks Unified Information Technology (NAMBUIT) cloud accounting platform. While cloud accounting offers advantages like real-time data access and reduced IT costs, it also introduces significant cybersecurity risks that can disrupt operations and damage customer trust. The study, combining quantitative analysis and literature review, found that current cybersecurity measures offer some protection but are insufficient to fully address the threats. It emphasizes the need for stronger cybersecurity frameworks, ongoing employee training, and enhanced regulatory compliance to secure the operations of MFBs. The findings highlight the importance of balancing the adoption of innovative cloud technologies with improved cybersecurity practices to ensure the growth and security of the microfinance sector in Nigeria. Recommendations include improving cybersecurity measures and aligning them better with regulatory standards.

Aminu (2024) examined the influence of cybersecurity measures on the financial performance of listed food and beverage companies in Nigeria. The study aimed to investigate the relationship between investments in cybersecurity and key financial indicators such as profitability, operating expenses, shareholder value, and regulatory compliance. Using an ex-post facto research design and primary data collected through structured questionnaires, the study applied multiple regression analysis to assess the impact of cybersecurity measures. The results revealed that cybersecurity measures and regulatory compliance significantly enhance financial performance, with cybersecurity investments also boosting shareholder value. However, while cybersecurity breaches were found to have a negative correlation with performance, they did not significantly affect financial outcomes. The study concludes that investing in robust cybersecurity frameworks and adhering to regulations is vital for the financial sustainability of Nigeria’s food and beverage sector.

Samoei and Gatobu (2024) assessed the effect of cybersecurity on the performance of internet banking services in commercial banks in Nairobi City County. The study employed a descriptive research design, surveying 38 licensed commercial banks in the region using a structured questionnaire. Data was analyzed using the Statistical Software for Social Sciences (SPSS), and the results were presented in tabular form. The study found that application security and IT governance are key factors influencing the performance of internet banking services. The authors recommend that commercial banks enhance the security of their mobile banking applications to protect customer data and funds from cyber threats. Suggestions include integrating additional security features such as fingerprint recognition and two-factor authentication (2FA).

Nwankwo, Kanyangale, Anoke, and Eze (2023) investigated the impact of cybersecurity on the business sustainability of listed microfinance banks in Nigeria. The study targeted 315 employees across three microfinance banks and adopted a census approach due to the manageable size of the population. Data was collected through a semi-structured questionnaire, and multiple regression analysis was used to test the hypotheses. The study found that cybersecurity significantly and positively impacts the sustainability of MFBs, with data availability being the most crucial factor, followed by data confidentiality and integrity. Employees emphasized that these cybersecurity elements are essential for sustaining their organizations. Based on these findings, the study urges MFBs to regularly review and strengthen their risk management strategies, adopting a more integrated approach to cybersecurity that combines technological solutions with human factors to address present and future cyber risks and build consumer trust in digital financial transactions.

Fatoki (2023) examined how cybersecurity influences financial fraud in Nigerian banks, focusing on the types of electronic fraud, the reasons behind cyber fraud, the challenges in preventing it, its impact on banks, and possible solutions. The study surveyed employees from six Nigerian banks, with a sample of 557 staff members selected using multistage sampling. A structured questionnaire was used to collect responses, which were analyzed using the SPSS statistical package. The study revealed that common types of cyber fraud in the banking system include computer viruses, hacking, phishing, pharming, and internal fraud by employees. Factors contributing to cybercrime include a lack of oversight, business pressures to meet targets, collusion between employees and outsiders, inadequate data encryption, and the use of third-party services. The study also identified several challenges impeding the prevention of cyber fraud, including the absence of national standards, insufficient infrastructure, internet vulnerabilities, and low customer awareness.

Austin-Olowo, Anike, and Ailemen (2023) explored various cybersecurity challenges impacting online banking and transactions in Nigeria, aiming to enhance the resilience of the financial system against these risks. The study employed both primary and secondary data to examine both old and new trends in cybersecurity related to online banking and transactions. The findings highlighted issues such as account hacking and delays in fund transfers between banks, which affect the efficiency of online banking in Nigeria. The research concluded that robust security measures are crucial for the success of online banking and transactions, particularly in Nigeria, to support economic growth. To address cybersecurity gaps, the study recommended increasing capacity-building programs, organizing sensitization seminars, hiring penetration testers, and conducting regular system upgrades.

Akintoye, Ogunode, Ajayi, and Joshua (2022) investigated the role of cybersecurity in fostering financial innovation within Nigerian Deposit Money Banks. With the rapid population growth and the challenge of reducing financial exclusion, there is an increasing need for financial innovation in the banking sector. However, factors such as poor design, vulnerabilities, and inconsistent adoption of new financial technologies have hindered progress. The study used a survey research design and gathered primary data from a sample of fifty-six staff members from various key departments in selected banks, which represented 93% of the total market capitalization as of December 31, 2021. The data were analyzed using both descriptive and inferential statistics. The findings revealed a significant positive impact of cybersecurity practices, particularly risk management and monitoring, on financial innovation in Nigerian banks (Adjusted R² = 0.447, F(2, 55) = 23.274, p < 0.05).

Khalil, Manzoor, Tahir, Khan, and Jamal (2021) investigated how cybersecurity costs influence the financial performance of e-banking, focusing on the mediating role of product innovation performance. The study's objectives included analyzing the relationship between various cybersecurity costs (prevention and detection, response, development, and indirect costs) and e-banking product innovation and financial performance, as well as exploring the mediating role of product innovation performance. The sample comprised managerial staff from various e-banks in Pakistan. The study utilized multivariate statistical techniques to analyze the data. The results indicated that prevention, response, and development costs significantly impacted product innovation performance and e-banking financial performance, while indirect costs had a negative effect. Additionally, product innovation performance was found to partially mediate the relationship between certain cybersecurity costs and financial performance, though it did not mediate the relationship between indirect costs and financial performance.

Ehioghiren, Ojeaga, and Eneh (2021) assessed cybersecurity from the perspective of accounting professionals in Nigeria. The study used a survey research design with a sample of 160 respondents from 148 auditing firms in Edo State. The hypotheses were tested using the F-test statistics and SPSS software. The findings indicated that accounting professionals in Nigeria are well-informed about cybersecurity and its related incidents within auditing firms. The study concluded that despite the increasing attention cybersecurity is receiving, more comprehensive planning and legislation are needed to address potential risks. It recommended stronger cybersecurity policies and frameworks to protect the digital space and encourage firms to adopt cybersecurity strategies to combat cybercrime, ultimately improving the knowledge of accounting professionals and providing guidance for policymakers.

Anoke, Igwebuike, Agagbo Ogugua, and Odumuato (2021) examined the impact of cybersecurity on the business sustainability of listed insurance firms in Nigeria. The study used a sample of 315 respondents from three listed insurance firms, with a questionnaire as the primary data collection tool. Simple linear regression was applied to test the hypotheses. The results showed a strong positive relationship between cybersecurity and the sustainability of listed insurance firms in Nigeria. The study concluded that cybersecurity is a critical strategy for ensuring the long-term viability of insurance firms. Recommendations included the implementation of stronger, enforceable cybersecurity laws to support the efforts of insurance firms in combating cybercrime, which would, in turn, enhance the sustainability of the industry.

# 2.4 Gap in Literature

While existing literature provides substantial perspectives on the relationship between cybersecurity and organizational performance across various financial sectors, a focused analysis of how financial loss from cybersecurity threats specifically affects earnings per share (EPS) in listed commercial banks in Nigeria remains largely underexplored. For instance, Anaege, Eneh, Inweregbu, and Okwuego (2025) examined cybersecurity threats in the context of operational efficiency in microfinance banks, while Aminu (2024) focused on cybersecurity investments and overall financial performance in the food and beverage sector. Similarly, Nwankwo, Kanyangale, Anoke, and Eze (2023) assessed the role of cybersecurity in the sustainability of microfinance banks, but did not delve into shareholder-specific indicators like EPS. Samoei and Gatobu (2024) addressed cybersecurity’s influence on internet banking services, and Fatoki (2023) centered on the impact of cybersecurity on financial fraud in Nigerian banks without quantifying the financial loss in terms of performance metrics like EPS. Furthermore, Austin-Olowo, Anike, and Ailemen (2023) studied online transaction risks, and Akintoye, Ogunode, Ajayi, and Joshua (2022) explored cybersecurity’s role in fostering financial innovation, while Khalil, Manzoor, Tahir, Khan, and Jamal (2021) assessed cybersecurity costs in relation to innovation and financial performance, but not EPS in the banking sector. Although Ehioghiren, Ojeaga, and Eneh (2021) and Anoke, Igwebuike, Agagbo Ogugua, and Odumuato (2021) explored cybersecurity from professional and insurance perspectives respectively, none of these studies directly analyzed the effect of financial loss due to cybersecurity threats on earnings per share within the Nigerian banking context. This reveals a significant gap in empirical literature, particularly in understanding how cybersecurity-related financial losses influence shareholder returns in listed commercial banks, thus justifying the need for this study.

# 3.0 Methodology

This study adopts an ex-post facto research design, which is suitable for investigating events that have already occurred without any manipulation or intervention by the researcher. The use of ex-post facto design is justified by the nature of the variables under consideration, particularly financial performance indicators and cybersecurity-related financial losses, which are historical and documented in publicly available financial records. Moreover, this design is cost-effective, less time-consuming, and appropriate for establishing cause-and-effect relationships in retrospective studies.

The population of the study comprises all fourteen (14) listed commercial banks (Deposit Money Banks) on the Nigerian Exchange Limited (NGX) as at December 2023. From this population, a sample of ten (10) listed commercial banks will be selected using judgmental sampling technique. This non-probability sampling approach is appropriate for selecting banks based on their availability of consistent annual reports, exposure to digital banking platforms, and record of cybersecurity incidents and losses over the study period. Banks selected must have published comprehensive financial statements and disclosed cybersecurity-related events or incidents for the period under study. The list of sample size is shown below in Table 1.

**Table 1 Sample Size**

|  |
| --- |
| 1. Access |
| 1. Fcmb |
| 1. Fidelity |
| 1. First Bank |
| 1. Gtco |
| 1. Stanbic Ibtc |
| 1. Sterling |
| 1. Uba |
| 1. Wema |
| 1. Zenith |

Source: Researcher’s Compilation (2025)

Data for the study were obtained from secondary sources, particularly the audited annual financial statements of the sampled banks, Nigeria Deposit Insurance Corporation annual reports and Nigeria Inter-Bank Settlement System fraud reports from 2012 to 2023. The study period was selected to align with the post-adoption phase of the International Financial Reporting Standards (IFRS), which became mandatory for publicly listed companies in Nigeria from 2012.

The independent variable — cybersecurity threat — was proxied by financial loss resulting from cybersecurity breaches, measured in monetary value (naira). The dependent variable is Earnings per Share (EPS), which is extracted directly from the banks’ annual financial statements. EPS is selected as it directly reflects shareholder value and is a key indicator of financial performance. In addition, Return on Assets (ROA) was included in the model as a control variable, representing the overall operational efficiency of the bank in utilizing its assets to generate income.

In addition to the descriptive analysis of the data using measures of central tendency and measures of dispersion, hypothesis testing was conducted using robust least square regression, which allows for estimating the effect of cybersecurity threats on financial performance while accounting for non-normality as well as heteroskedasticity. Hypothesis testing was conducted at a 5% significance level. The null hypothesis is rejected if the p-value is less than 0.05 while the alternate hypothesis is accepted and vice versa.

The model for the study is designed to reflect the relationship between financial losses due to cybersecurity threats and the earnings per share (EPS) of listed commercial banks, while controlling for other relevant variables such as firm size and ROA.

Functional Forms of the Model

EPS = f(CYB, ROA)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_eq1

Econometric Expressions

EPSt = β₀ + β₁CYBt + β₂ROAt + μt\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_eq2

Where:

* EPS = Earnings per Share
* ROA = Return on Assets
* CYB = Financial loss due to cybersecurity threat
* t = year in question
* β₀ = Constant term
* β₁, β₂ = Coefficients of explanatory variables
* μ = Error term capturing omitted variables and unobserved heterogeneity

# 4.0 Result and Discussion

# 4.1 Descriptive Analysis

**Table 2 Descriptive Analysis**

|  |  |  |  |
| --- | --- | --- | --- |
|  | EPS | CYB | ROA |
|  |  | ₦’b |  |
| Mean | 2.688779 | 11.09750 | 0.036091 |
| Median | 1.630000 | 8.905000 | 0.017650 |
| Maximum | 19.07000 | 40.00000 | 0.325404 |
| Minimum | -0.420000 | 2.370000 | -0.020515 |
| Std. Dev. | 3.508782 | 10.27387 | 0.057151 |
| Skewness | 2.821038 | 1.694550 | 3.251809 |
| Kurtosis | 12.24103 | 5.493860 | 13.60411 |
| Jarque-Bera | 586.1486 | 88.52668 | 773.7214 |
| Probability | 0.000000 | 0.000000 | 0.000000 |
| Sum | 322.6535 | 1331.700 | 4.330862 |
| Sum Sq. Dev. | 1465.074 | 12560.74 | 0.388677 |
| Observations | 120 | 120 | 120 |

Source: Eviews 10 Output (2025)

Earnings Per Share (EPS) as shown in Table 2 has a mean value of 2.69, indicating that, on average, listed commercial banks in Nigeria generated earnings of approximately ₦2.69 per share during the study period (2012–2023). The maximum EPS recorded was ₦19.07, while the minimum dropped to ₦-0.42, suggesting that at least one bank experienced a net loss per share in a given year. The standard deviation of 3.51 reflects considerable variation in earnings performance across the sampled banks, which may be attributable to differences in operational efficiency, risk management practices, and exposure to cybersecurity threats. The distribution of EPS is positively skewed (2.82), implying a long right tail—meaning that a few banks had exceptionally high EPS values, skewing the average upward. The kurtosis value of 12.24 exceeds the normal value of 3, indicating a leptokurtic distribution with heavy tails and a sharp peak, suggesting more frequent extreme values than a normal distribution. The Jarque-Bera probability value of 0.0000 confirms that the distribution of EPS is not normally distributed, which justifies the use of robust least squares regression that accounts for non-normality in hypothesis testing.

Cybersecurity Threat (CYB), proxied by financial losses due to cyber breaches, shows a mean value of ₦11.10 billion, suggesting that Nigerian commercial banks recorded average annual cybersecurity-related financial losses of over ₦11 billion during the study period. The maximum reported loss was ₦40 billion, while the minimum was ₦2.37 billion, reflecting wide variability in the severity of cyber incidents across institutions and years. The standard deviation of ₦10.27 billion highlights a substantial dispersion from the mean, reinforcing that cybersecurity threats have an uneven impact depending on each bank’s vulnerability, digital infrastructure, and response mechanisms. The skewness of 1.69 shows a right-skewed distribution, indicating that most banks experienced losses lower than the mean, but a few faced exceptionally large losses. The kurtosis of 5.49 further signals a leptokurtic distribution, meaning the data has heavy tails and potential outliers—banks with extreme losses. The Jarque-Bera probability value of 0.0000 suggests that the data does not follow a normal distribution, affirming the relevance of robust estimation techniques for regression analysis.

Return on Assets (ROA), used as a control variable in the study, has a mean value of 0.0361 (or 3.61%), which indicates that on average, banks generate a return of ₦3.61 on every ₦100 worth of assets employed. The maximum ROA is 32.54%, while the minimum is -2.05%, suggesting that while some banks were highly efficient, others experienced negative asset returns, possibly due to operational inefficiencies, non-performing loans, or financial disruptions from cybersecurity breaches. The standard deviation of 0.0572 implies a relatively modest spread in asset efficiency compared to EPS and CYB. However, the skewness of 3.25 indicates a high degree of right skewness, meaning a few banks reported exceptionally high ROAs. The kurtosis value of 13.60 signifies a leptokurtic distribution, indicating a sharp peak with fat tails, again pointing to a tendency toward extreme values. The Jarque-Bera probability of 0.0000 confirms that ROA data is non-normally distributed, further reinforcing the methodological choice to use robust least squares regression to address potential heteroskedasticity and distributional issues in the data.

# 4.2 Test of Hypothesis

H01: Financial losses from cybersecurity threat do not significantly affect the earnings per share of listed commercial banks in Nigeria.

**Table 3 Test of Hypotheses**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Dependent Variable: EPS | | |  |  |
| Method: Robust Least Squares | | |  |  |
| Date: 03/30/25 Time: 22:07 | | |  |  |
| Sample: 1 120 | |  |  |  |
| Included observations: 120 | | |  |  |
| Method: M-estimation | | |  |  |
| M settings: weight=Fair, tuning=1.4, scale=MAD (median centered) | | | | |
| Huber Type I Standard Errors & Covariance | | | |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Variable | Coefficient | Std. Error | z-Statistic | Prob. |
|  |  |  |  |  |
|  |  |  |  |  |
| CYB | -0.013024 | 0.001314 | -9.909912 | 0.0000 |
| ROA | 15.02042 | 0.236253 | 63.57771 | 0.0000 |
| C | 1.349862 | 0.021418 | 63.02489 | 0.0000 |
|  |  |  |  |  |
|  |  |  |  |  |
|  | Robust Statistics | |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Rw-squared | 0.139425 | Adjust Rw-squared | | 0.139425 |
| Scale | 1.553870 | Rn-squared statistic | | 4180.964 |
| Prob(Rn-squared stat.) | 0.000000 |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Source: Eviews 10 Output (2025)

As shown in Table 3 above, the robust R-squared (Rw-squared) value of 0.1394 implies that about 13.94% of the variation in EPS across listed commercial banks is explained by the combined effects of financial losses from cybersecurity threats (CYB) and return on assets (ROA). Although this percentage may appear modest, it is meaningful in financial studies, especially where other unobservable factors also influence profitability. The model’s Prob(Rn-squared stat.) is 0.000000, indicating that the overall model is statistically significant at the 1% level. This confirms that the explanatory variables jointly have a significant effect on the dependent variable (EPS), validating the robustness of the model in explaining how cybersecurity threats and asset performance affect bank earnings.

The coefficient for ROA is 15.02042, which means that a 1 unit increase in ROA (or 100% increase in asset efficiency) will lead to an approximate ₦15.02 increase in EPS. This shows a strong positive marginal effect, indicating that better utilization of bank assets directly enhances shareholder returns. Even smaller increments in ROA would still have meaningful effects on EPS. The p-value is 0.0000, confirming that this effect is also statistically significant at the 5% level. Although ROA is not the primary variable of interest in this study, its significant positive effect validates its inclusion as a control variable, helping to isolate the true effect of cybersecurity threats on EPS.

The constant term (C) in the model is 1.349862, suggesting that when both cybersecurity losses (CYB) and return on assets (ROA) are held constant at zero, the base level of earnings per share would be approximately ₦1.35. While this constant has limited interpretive value on its own, it provides a mathematical anchor for the regression model. The p-value of 0.0000 indicates that the intercept is statistically significant, meaning it contributes meaningfully to the overall model specification.

The coefficient of CYB (Cybersecurity Threat), proxied by financial loss in naira, is -0.013024, which implies that for every ₦1 billion increase in financial loss due to cybersecurity breaches, the Earnings Per Share (EPS) of listed commercial banks in Nigeria decreases by ₦0.013. This reflects a negative marginal effect, showing that cybersecurity-related financial losses erode shareholder value. More specifically, as cybersecurity losses increase, the amount available to be distributed per share declines, reducing profitability on a per-share basis. The effect is statistically significant at the 5% level since the p-value is 0.0000, which is less than the 0.05 threshold. Thus, the study provides strong evidence that financial losses resulting from cybersecurity threats significantly reduce the earnings per share of Nigerian commercial banks over the study period. Having accepted the alternate hypothesis, it implies that Financial losses from cybersecurity threats have a negative effect on the earnings per share of listed commercial banks in Nigeria (β = -0.013024, p = 0.0000).

# 4.3 Discussion of Finding

The finding that financial losses from cybersecurity threats have a negative and statistically significant effect on the earnings per share (EPS) of listed commercial banks in Nigeria (β = -0.013024, p = 0.0000) is both theoretically sound and empirically supported. Cybersecurity breaches often result in direct financial losses—such as theft, fraud, and fines—as well as indirect consequences like reputational damage, customer attrition, and increased compliance costs. All of these effects inevitably reduce the net income available to shareholders, thereby shrinking EPS. This result is particularly relevant for the banking sector, where trust, data integrity, and operational resilience are paramount for maintaining investor confidence and profitability. It also reflects how financial losses from cyber incidents are not just IT issues but have tangible economic consequences, influencing core performance metrics like EPS. The study by Fatoki (2023) aligns with this conclusion, revealing that Nigerian banks suffer various forms of cyber fraud—such as phishing, hacking, and insider collusion—that directly impact financial performance, although his study focuses on fraud types rather than financial outcome metrics like EPS. Similarly, Austin-Olowo et al. (2023) found that cybersecurity challenges such as hacking and interbank transaction delays significantly affect online banking, indirectly affirming that cyber threats can erode earnings and operational efficiency. Anaege et al. (2025), while focused on microfinance banks, emphasized that existing cybersecurity frameworks are insufficient, often leading to disruptions and loss of stakeholder trust—factors that likely contribute to decreased performance, mirroring the findings in this study. On the other hand, Aminu (2024) presents a nuanced view: although he reports a negative correlation between cybersecurity breaches and financial performance in food and beverage firms, the relationship was not statistically significant in that context. This contrast may stem from sectoral differences, as the banking industry is more data-intensive and reputation-sensitive than manufacturing sectors, making it more vulnerable to the performance effects of cyber incidents. Together, these studies offer a balanced empirical context, reinforcing the credibility and sector-specific relevance of the present findings.

# 5.0 Conclusion and Recommendation

Commercial banks operating within a secure digital infrastructure ensure the confidentiality, integrity, and availability of financial data and services. Thus is because such an environment promotes customer confidence, enhances operational efficiency, and drives financial performance through seamless transactions and uninterrupted service delivery. With strong cybersecurity frameworks in place, financial institutions are expected to detect, prevent, and respond to cyber threats proactively, thereby minimizing risks and safeguarding stakeholder interests. This is possible only when cybersecurity is integrated into corporate governance, risk management, and strategic planning, resulting in increased profitability, regulatory compliance, and long-term sustainability.

The findings of this study have significant implications for the financial sector in Nigeria, particularly for listed commercial banks. The negative effect of financial losses from cybersecurity threats on earnings per share (EPS) highlights the economic vulnerability that banks face in an increasingly digital environment. As cyberattacks become more sophisticated and pervasive, their ability to disrupt operations, compromise customer data, and damage a bank's reputation becomes more pronounced. This study underscores how cybersecurity risks are not just technical or operational challenges but also crucial financial concerns that directly affect the bottom line. For investors, this means that banks with poor cybersecurity risk management practices may face diminished shareholder returns due to these unexpected financial losses, making cybersecurity a critical factor in evaluating the financial health of banks.

Based on the findings, the following recommendations can be made:

1. For Bank Management: To mitigate the negative effect of cybersecurity threats on earnings per share, it is crucial for the management of listed commercial banks in Nigeria to prioritize investment in robust cybersecurity frameworks by implementing advanced security measures and proactive risk management strategies to minimize financial losses resulting from cyber incidents, safeguarding the bank's financial performance.

2. For Investors: Given the negative impact of cybersecurity threats on earnings, investors should incorporate cybersecurity risk assessments into their decision-making processes when evaluating potential investments in Nigerian commercial banks. By considering the cybersecurity practices of banks, investors can better anticipate the financial stability and growth potential of their investments.

# 5.1 Limitation of the Study and Suggestion for Further Studies

A key constraint of this research lies in its focus on only 10 of the 14 commercial banks listed on the Nigerian Exchange, which may limit the generalizability of the results across the entire banking sector. The application of a judgmental sampling method may also introduce some degree of selection bias, as the banks chosen may not fully reflect the diversity of cybersecurity experiences within the industry. Furthermore, the study relies solely on secondary data sources—mainly published financial statements and government records—which may not adequately reflect the complexities or full extent of cybersecurity incidents and their associated financial consequences. Additionally, the analysis was restricted to the influence of cybersecurity-related financial losses on earnings per share, thereby narrowing the perspective on how such threats might impact other dimensions of financial performance.

Subsequent studies may consider expanding the scope to include all 14 listed commercial banks or incorporate other financial institutions such as microfinance banks, which may encounter unique cybersecurity risks. Future research could also benefit from examining the influence of cybersecurity threats on additional financial metrics, such as return on assets (ROA) or return on equity (ROE), to provide a more holistic view of their financial implications. Moreover, incorporating primary data through structured interviews or surveys with bank executives, IT personnel, and cybersecurity professionals could offer more hints into how financial institutions identify, manage, and respond to cybersecurity threats in real time.

Disclaimer (Artificial intelligence)

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc.) and text-to-image generators have been used during the writing or editing of this manuscript.

# References

Aggreh, M., Abiahu, M. C., & Nworie, G. O. (2023). Cost reduction and financial performance of listed consumer goods firms in Nigeria. *Journal of Banking*, *11*(1), 1-38.

Akintoye, R., Ogunode, O., Ajayi, M., & Joshua, A. A. (2022). Cyber security and financial innovation of selected deposit money banks in Nigeria. *universal Journal of Accounting and Finance*, *10*(3), 643-652.

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

Aminu, M. A. (2024). Effect Of Cyber Security Measures On Financial Performance In Listed Food And Beverage Companies In Nigeria. *ANUK College of Private Sector Accounting Journal*, *1*(2), 232-242.

Anaege, A. E., Eneh, O. M., Inweregbu, O. A., & Okwuego, S. P. (2025). Cybersecurity threats in cloud accounting: A case study of microfinance banks in Anambra State using NAMBUIT banking software. *International Journal of Research and Innovation in Applied Science (IJRIAS)*, *X*(III), 290.

Anoke, A. F., Igwebuike, J., Agagbo Ogugua, C., & Odumuato, V. (2021). Cyber Security and Business Sustainability of Quoted Insurance Firms in Nigeria. *Journal of Research in Business and Management*, *9*(12), 16-22.

Arsal, M. (2021). Impact of earnings per share and dividend per share on firm value. *ATESTASI: Jurnal Ilmiah Akuntansi*, *4*(1), 11-18.

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

Ayuba, H., Bambale, A. J. A., Ibrahim, M. A., & Sulaiman, S. A. (2019). Effects of Financial Performance, Capital Structure and Firm Size on Firms' Value of Insurance Companies in Nigeria. *Journal of Finance, Accounting & Management*, *10*(1).

Bose, I., & Leung, A. C. M. (2024). Cybersecurity Investments and Financial Performance: Evidence from Global Banks. *Information Systems Research, 35*(1), 112-130.

Ehioghiren, E. E., Ojeaga, J. O., & Eneh, O. (2021). Cyber security: The perspective of accounting professionals in Nigeria. *Accounting and taxation review*, *5*(2), 15-29.

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.

Gartenberg, C., Prat, A., & Serafeim, G. (2019). Corporate purpose and financial performance. *Organization Science*, *30*(1), 1-18.

Hermanson, D. R., & Wolfe, D. T. (2024). The Fraud Diamond. *CPA Journal*, *94*.

Jang-Jaccard, J., & Nepal, S. (2022). A Survey of Emerging Threats in Cybersecurity and Risk Management Frameworks. *Journal of Computer Security, 30*(2), 183-208.

Khalil, K., Manzoor, S. R., Tahir, M., Khan, N., & Jamal, K. (2021). Impact of Cyber Security Cost on the Financial Performance of E-Banking: Mediating Influence of Product Innovation Performance. *Humanities & Social Sciences Reviews*, *9*(2), 691-703.

Kshetri, N. (2023). Cybersecurity in the Banking Sector: Challenges and Opportunities in Emerging Economies. *Journal of International Business Studies, 54*(5), 876-892.

Kumar, P. (2017). Impact of earning per share and price earnings ratio on market price of share: a study on auto sector in India. *International Journal of Research*, *5*(2), 113-118.

Mansor, N., & Abdullahi, R. (2015). Fraud triangle theory and fraud diamond theory. Understanding the convergent and divergent for future research. *International Journal of Academic Research in Accounting, Finance and Management Science*, *1*(4), 38-45.

Mansor, R. A. N. (2015). Forensic accounting and fraud risk factors: the influence of fraud diamond theory. *The American Journal of Innovative Research and Applied Sciences*, *7*(28), 186-192.

Nigeria Inter-Bank Settlement System. (2024). *2023 Annual Fraud Landscape*. <https://nibss-plc.com.ng/wp-content/uploads/2024/04/2023-Annual-Fraud-Landscape.pdf>

Nwafor, V. O., & Nworie, G. O. (2025). Risk management in Nigerian listed commercial banks: The significance of board composition (2013–2023). *International Journal of Financial, Accounting, and Management, 6*(4), 525–543.

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

Nworie, G. O., Moedu, V. O., & Onyali, C. I. (2023). Contribution of current assets management to the financial performance of listed consumer goods firms in Nigeria. *International Journal of Trend in Scientific Research and Development*, *7*(1), 77-87.

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

Raveendra, P. V., Singh, J. E., Singh, P., & Kumar, S. S. (2018). Behavioral finance and its impact on poor financial performance of SMEs: A review. *International Journal of Mechanical Engineering and Technology*, *9*(5), 341-348.

Samoei, P. C., & Gatobu, P. (2024). Cybersecurity and Performance of Internet Banking Services in Commercial Banks in Nairobi City County, Kenya. *International Journal of Social Sciences Management and Entrepreneurship (IJSSME)*, *8*(1).