CSCanada
Cross-Cultural Communication
Vol. 21, No. 3, 2025, pp. 41-50
DOI:10.3968/13849

ISSN 1712-8358[Print]
ISSN 1923-6700[Online]
www.cscanada.net
www.cscanada.org

Cyber Security and Its Implications on Financial Fraud in Deposit Money Banks in Yenagoa Metropolis, Bayelsa State

Fawei Enifie James[a],*

[a] Department of Sociology, Faculty of Social Sciences, Niger Delta University, Wilberforce Island, Nigeria.
*Corresponding author.

Received 2 August 2025; accepted 16 September 2025
Published online 26 September 2025

Abstract

This study examines the critical role of cyber security in mitigating financial fraud within deposit money banks in Yenagoa Metropolis, Bayelsa State. As digital banking platforms proliferate, the increasing sophistication of cyber-attacks poses significant threats to financial institutions, compromising customer trust and economic stability. This research investigates the prevalence, nature, and implications of cyber-enabled financial fraud, focusing on the vulnerabilities exploited in banking systems and their economic consequences. Employing a mixed-methods approach, data were collected through surveys and interviews with bank officials, cybersecurity experts, and customers, alongside an analysis of reported fraud cases. Findings reveal that weak authentication protocols, phishing attacks, and insider threats are primary conduits for financial fraud, exacerbated by inadequate cybersecurity infrastructure and low digital literacy among customers. The study underscores the urgent need for robust cybersecurity frameworks, including advanced encryption, multi-factor authentication, and regular staff training, to safeguard financial transactions. Furthermore, it highlights the necessity for collaborative efforts between banks, regulatory bodies, and technology providers to enhance resilience against cyber threats. The implications of these findings suggest that strengthening cybersecurity measures not only reduces financial losses but also fosters customer confidence and regulatory compliance. This research contributes to the discourse on securing financial systems in emerging economies, offering actionable recommendations for policymakers and banking institutions in Yenagoa Metropolis to combat cyber-enabled financial fraud effectively.

Key words: Cyber Security; Financial Fraud; Deposit Money Banks; Yenagoa; Implications

James, F. E. (2025). Cyber Security and Its Implications on Financial Fraud in Deposit Money Banks in Yenagoa Metropolis, Bayelsa State. *Cross-Cultural Communication, 21*(3), 41-50. Available from: http//www.cscanada.net/index.php/ccc/article/view/13849
DOI: http://dx.doi.org/10.3968/13849

1. INTRODUCTION

In the rapidly evolving digital landscape, the banking sector has increasingly adopted technological advancements to enhance service delivery and operational efficiency. Deposit money banks (DMBs) in Yenagoa Metropolis, Bayelsa State, a critical hub for economic activities, have embraced these innovations to streamline operations and improve customer experiences. However, this digital transformation has exposed DMBs to a growing array of sophisticated cybersecurity threats and cybercrimes, including phishing attacks, ransomware, identity theft, and social engineering tactics (Okeshola & Adeta, 2019). These threats exploit vulnerabilities in digital infrastructure and human factors, enabling cybercriminals to perpetrate financial fraud with far-reaching consequences. In Nigeria, the financial sector incurs annual losses of approximately USD 500 million due to cybercrime, with urban centers like Yenagoa being particularly vulnerable to phishing, hacking, and electronic fraud (Omodunbi et al., 2020). These incidents undermine customer trust, result in significant financial losses, and challenge the integrity of the banking system. The situation is worsened by inadequate cybersecurity measures, insufficient employee training, and limited awareness of cyber threats among both staff

and customers, which create exploitable loopholes that hinder timely detection and prevention of fraudulent activities. This article examines the predominant cybersecurity threats and cybercrimes affecting DMBs in Yenagoa, Bayelsa State, and explores how deficiencies in cybersecurity frameworks, training, and awareness contribute to the persistence and detection of financial fraud. By highlighting these critical issues, the article underscores the urgent need for robust cybersecurity strategies to safeguard the financial ecosystem in Yenagoa Metropolis and foster resilience against the evolving landscape of cyber threats.

2. STATEMENT OF THE PROBLEM

The proliferation of digital banking services in Nigeria has coincided with a surge in cybercrimes, with deposit money banks in Yenagoa, Bayelsa State, being no exception. Recent studies highlight that Nigerian banks face sophisticated cyber threats, including phishing, pharming, identity theft, SIM swap fraud, and skimming, which collectively contribute to substantial financial losses estimated at N273 billion in 2022 alone. These cybercrimes exploit vulnerabilities in banking systems, often resulting in unauthorised access to customer accounts, data breaches, and fraudulent transactions. In Yenagoa, a rapidly developing metropolis with increasing adoption of internet banking, the specific nature and impact of these threats remain underexplored due to the focus of existing research on larger urban centres. This geographical gap in the literature limits the understanding of how regional socio-economic and infrastructural factors influence cybersecurity challenges in smaller cities like Yenagoa.

Inadequate cybersecurity measures, such as weak encryption, outdated systems, and insufficient security audits, exacerbate the vulnerability of DMBs to cyber-attacks. Studies indicate that many Nigerian banks struggle with misconfigurations and lack robust compliance with regulatory frameworks, increasing the risk of breaches. In Yenagoa, where technological infrastructure may lag behind national financial hubs, these deficiencies are likely amplified, yet there is a paucity of empirical data addressing this context. Furthermore, insufficient employee training on emerging cyber threats, such as social engineering and ransomware, undermines the ability of bank staff to detect and mitigate risks effectively. Research suggests that human error, often due to inadequate training, accounts for approximately 88% of cybersecurity incidents in the financial sector. This issue is particularly critical in Yenagoa, where limited access to advanced cybersecurity training programmes may hinder the development of a robust cybersecurity culture among bank employees.

Limited awareness of cyber threats among both employees and customers further complicates fraud detection and prevention. In Nigeria, phishing attacks have surged, with over 1.3 million attempts recorded in the first half of 2023, targeting bank customers through deceptive tactics. In Yenagoa, low financial literacy and cultural tendencies to trust authority figures may heighten susceptibility to social engineering attacks, yet there is little research exploring how these socio-cultural factors influence cybersecurity awareness in the region. The absence of targeted public awareness campaigns tailored to the local context further perpetuates this challenge, leaving customers vulnerable to fraud and banks struggling to maintain trust.

The literature also reveals gaps in understanding the interplay between cybersecurity deficiencies and financial fraud in regional settings. While studies like Fatoki (2023) have examined cybersecurity's influence on financial fraud in Nigeria's banking sector, they often adopt a national perspective, overlooking regional variations. Similarly, research on cybersecurity practices in Nigerian banks tends to focus on technical solutions, with less attention to the role of employee training and customer education in fraud prevention. The lack of comprehensive studies specific to Yenagoa creates a critical knowledge gap, as the city's unique socio-economic dynamics, including its oil-driven economy and relatively nascent digital infrastructure, may present distinct cybersecurity challenges.

This study seeks to address these gaps by investigating the primary cybersecurity threats and cybercrimes affecting DMBs in Yenagoa, their contribution to financial fraud, and the influence of inadequate cybersecurity measures, insufficient employee training, and limited awareness on fraud occurrence and detection. By providing a localised analysis, this research will contribute to the literature by offering insights into the cybersecurity landscape of a regional banking hub, informing policy and practice to enhance fraud prevention and cybersecurity resilience. The findings will also support the development of tailored interventions, such as region-specific training programmes and awareness campaigns, to mitigate cyber risks and foster a secure banking environment in Yenagoa.

3. RESEARCH QUESTIONS

• What are the primary cybersecurity threats and cybercrimes affecting deposit money banks in Yenagoa, Bayelsa State, and how do these contribute to financial fraud within the banking sector?

• To what extent do inadequate cybersecurity measures, insufficient employee training, and limited awareness of cyber threats influence the occurrence and detection of financial fraud in deposit money banks in Yenagoa, Bayelsa State?

4. RESEARCH OBJECTIVES

• To identify and analyse the primary cybersecurity threats and cybercrimes impacting deposit money banks in Yenagoa, Bayelsa State, and evaluate their role in facilitating financial fraud within the banking sector.

• To examine the extent to which inadequate cybersecurity measures, insufficient employee training, and limited awareness of cyber threats contribute to the occurrence and hinder the detection of financial fraud in deposit money banks in Yenagoa, Bayelsa State.

5. RESEARCH HYPOTHESES

• **H0**: There is no significant relationship between cybersecurity threats and cybercrimes and the incidence of financial fraud in deposit money banks in Yenagoa, Bayelsa State.
· **H1**: There is a significant relationship between cybersecurity threats and cybercrimes and the incidence of financial fraud in deposit money banks in Yenagoa, Bayelsa State.

• **H0**: Inadequate cybersecurity measures, insufficient employee training, and limited awareness of cyber threats do not significantly influence the occurrence and detection of financial fraud in deposit money banks in Yenagoa, Bayelsa State.
· **H1**: Inadequate cybersecurity measures, insufficient employee training, and limited awareness of cyber threats significantly influence the occurrence and detection of financial fraud in deposit money banks in Yenagoa, Bayelsa State.

6. LITERATURE REVIEW

Conceptual Review

Cybersecurity in the banking sector refers to the measures and strategies employed to protect digital systems, networks, and sensitive financial data from unauthorized access, cyberattacks, and fraud. It encompasses technologies, policies, and practices designed to safeguard the confidentiality, integrity, and availability of information in Deposit Money Banks (DMBs). Financial fraud, on the other hand, involves deceptive tactics used to gain illicit financial benefits, often exploiting vulnerabilities in digital banking platforms. Common forms of cyber-enabled financial fraud in DMBs include phishing, malware attacks, identity theft, SIM swap fraud, and skimming. These threats exploit technological weaknesses, human errors, and inadequate internal controls, leading to significant financial losses and erosion of customer trust. In the context of Yenagoa Metropolis, Bayelsa State, the rapid adoption of digital banking services has heightened the need for robust cybersecurity frameworks to mitigate fraud risks, as banks increasingly rely on online platforms for transactions.

Theoretical Review

The study of cybersecurity and financial fraud in DMBs can be grounded in several theoretical frameworks, notably the Fraud Triangle Theory, Routine Activity Theory, and Protection Motivation Theory.

The **Fraud Triangle Theory** (Cressey, 1953) posits that fraud occurs due to three elements: pressure, opportunity, and rationalization. In DMBs, employees or external actors may face financial or non-financial pressures (e.g., meeting deposit targets or economic hardship), exploit opportunities (e.g., weak internal controls or unpatched systems), and rationalize their actions as justified.

The **Routine Activity Theory** (Cohen & Felson, 1979) suggests that cybercrime occurs when a motivated offender, a suitable target (e.g., vulnerable banking systems), and the absence of a capable guardian (e.g., weak cybersecurity measures) converge. This theory is relevant in explaining how cyber fraud thrives in environments with inadequate security protocols. The **Protection Motivation Theory** (Rogers, 1975) highlights how individuals or institutions adopt protective behaviors (e.g., implementing cybersecurity measures) based on perceived threats and the efficacy of countermeasures. These theories collectively provide a lens to understand the motivations, opportunities, and preventive strategies for combating financial fraud in DMBs in Yenagoa Metropolis.

Empirical Review

Recent studies have explored the nexus between cybersecurity and financial fraud in DMBs, particularly in Nigeria. Fatoki (2023) investigated the influence of cybersecurity on financial fraud in the Nigerian banking industry, identifying prevalent fraud types such as phishing, hacking, and pharming, driven by inadequate data encryption and insider collusion. The study emphasized the need for robust cybersecurity awareness programs to foster a security-conscious culture in banks. Similarly, Akintoye et al. (2022) found a significant positive relationship between cybersecurity measures (e.g., risk management and monitoring) and financial innovation in Nigerian DMBs, suggesting that effective cybersecurity enhances operational efficiency and reduces fraud risks. A study by OTUOGHA et al. (2021) in Bayelsa State revealed a weak positive correlation (21%) between internal audit practices and employee fraud, indicating that internal controls alone are insufficient without proactive cybersecurity measures. Furthermore, a 2024 study on Nigerian DMBs highlighted that cybersecurity audits significantly improve data protection, productivity, and customer trust, with AI-based auditing tools achieving a 93% fraud detection rate. These findings underscore the critical role of advanced cybersecurity strategies in mitigating financial fraud in DMBs, particularly in regions like Yenagoa Metropolis, where digital banking adoption is growing.

7. THEORETICAL FRAMEWORK

To investigate the implications of cyber security on financial fraud in deposit money banks in Yenagoa Metropolis, Bayelsa State, a robust theoretical framework is essential to provide a structured lens through which the relationship between cyber security measures and financial fraud can be analysed. The **Routine Activity Theory (RAT)** is proposed as a suitable framework for this study due to its applicability to cybercrime and its focus on the situational factors that facilitate criminal activities, including financial fraud in banking institutions.

Routine Activity Theory (RAT)

The Routine Activity Theory, developed by Cohen and Felson (1979), posits that for a crime to occur, three key elements must converge in time and space: (1) a motivated offender, (2) a suitable target, and (3) the absence of a capable guardian. This theory, originally developed to explain traditional crimes, has been widely adapted to study cybercrime due to its relevance in analysing the opportunities and vulnerabilities that enable criminal activities in digital environments.

Components of Routine Activity Theory

• **Motivated Offender**: In the context of cyber security and financial fraud, motivated offenders are cybercriminals who seek financial gain through fraudulent activities such as phishing, identity theft, or unauthorised access to bank systems. These individuals or groups are driven by the potential for monetary rewards and exploit weaknesses in cyber security systems.

• **Suitable Target**: Deposit money banks in Yenagoa Metropolis represent suitable targets due to their handling of large volumes of financial transactions and sensitive customer data. The digital infrastructure of banks, including online banking platforms and automated teller machines (ATMs), can be vulnerable to exploitation if not adequately protected, making them attractive to cybercriminals.

• **Absence of a Capable Guardian**: A capable guardian refers to mechanisms or measures that deter or prevent criminal activities. In the banking sector, capable guardians include robust cyber security measures such as firewalls, encryption, intrusion detection systems, and employee training on fraud prevention. The absence or inadequacy of these measures increases the likelihood of financial fraud.

Application of RAT to the Study

The Routine Activity Theory is highly relevant to the study of cyber security and its implications on financial fraud in deposit money banks in Yenagoa Metropolis for the following reasons:

• **Motivated Offenders in the Cyber Context**: The rise of digital banking has attracted cybercriminals who exploit vulnerabilities in online systems. RAT helps frame the motivations of these offenders, who target banks due to the potential for significant financial rewards. By understanding the incentives driving cybercriminals, banks can develop targeted strategies to disrupt their activities.

• **Suitable Targets in Banking Systems**: Banks in Yenagoa Metropolis, like many financial institutions, rely on digital platforms for transactions and customer interactions. RAT highlights how these platforms, if inadequately secured, become suitable targets for fraudsters. For instance, weak authentication protocols or outdated software can create opportunities for cybercriminals to perpetrate fraud.

• **Role of Capable Guardians**: RAT underscores the importance of effective cyber security measures as capable guardians. In the context of this study, the presence of strong cyber security frameworks—such as multi-factor authentication, real-time fraud detection systems, and regular security audits—can reduce the opportunities for financial fraud. The theory provides a basis for evaluating the effectiveness of existing cyber security measures in Yenagoa's banks and identifying gaps that need to be addressed.

Relevance to the Topic

The Routine Activity Theory aligns with the topic by providing a framework to analyse how cyber security measures (or their absence) influence the occurrence of financial fraud in deposit money banks. By examining the convergence of motivated offenders, suitable targets, and the absence of capable guardians, the theory enables a systematic exploration of the factors contributing to financial fraud in Yenagoa Metropolis. It also guides the identification of practical

8. METHODOLOGY FOR THE STUDY

This study adopted a descriptive survey research design to investigate the implications of cybersecurity on financial fraud in deposit money banks (DMBs) in Yenagoa Metropolis, Bayelsa State. The descriptive survey design was suitable as it allowed for the collection of data from a sample to describe the characteristics, perceptions, and experiences of the population concerning cybersecurity practices and financial fraud. The study employed both quantitative and qualitative methods to ensure a comprehensive analysis. Quantitative data were collected through structured questionnaires, while qualitative data were gathered through semi-structured interviews with key informants, such as bank managers and IT security personnel.

9. STUDY AREA

The study was conducted in Yenagoa Metropolis, the capital city of Bayelsa State, Nigeria. Yenagoa was a rapidly developing urban centre with a growing number

of deposit money banks servicing both individual and corporate clients. The choice of Yenagoa was justified by its economic significance in the Niger Delta region and the increasing adoption of digital banking services, which made it a relevant setting for studying cybersecurity challenges and financial fraud in the banking sector.

10. POPULATION OF STUDY

The population of the study comprised all employees and management staff of deposit money banks operating in Yenagoa Metropolis. According to the Central Bank of Nigeria, there were approximately eight licensed deposit money banks with branches in Yenagoa as of 2023, with an estimated total of 500 employees across these institutions. This population included bank tellers, customer service representatives, IT staff, and senior management, who were directly or indirectly involved in cybersecurity practices and fraud prevention.

11. SAMPLE SIZE AND SAMPLING TECHNIQUE

To determine the sample size, the study used the Taro Yamane formula for calculating sample size from a finite population, given its appropriateness for survey-based research. The formula was:

[n = \frac{N}{1 + N(e^2)}]

Where:

• (n) = Sample size

• (N) = Population size (500 employees)

• (e) = Margin of error (set at 0.05 for a 95% confidence level)

Substituting the values:

[n = \frac{500}{1 + 500(0.05^2)} = \frac{500}{1 + 500(0.0025)} = \frac{500}{1 + 1.25} = \frac{500}{2.25} \approx 222]

Thus, the sample size was approximately 222 respondents.

The study employed a stratified random sampling technique to ensure representation across different categories of bank employees (e.g., tellers, IT staff, and management). The population was stratified based on job roles, and a proportional number of respondents were randomly selected from each stratum to reflect the population's diversity.

12. DATA COLLECTION METHODS

Primary data were collected using:

• **Structured Questionnaires**: These were administered to the sampled employees to gather quantitative data on their awareness of cybersecurity measures, experiences with financial fraud, and perceptions of the effectiveness of existing controls.

• **Semi-Structured Interviews**: Conducted with 10-15 purposively selected senior bank staff and IT specialists to gain in-depth insights into cybersecurity strategies and challenges in fraud prevention.

Secondary data were sourced from audited financial statements, Central Bank of Nigeria reports, and relevant literature to provide context on cybersecurity and fraud trends.

13. DATA ANALYSIS

Quantitative data from questionnaires were analysed using Statistical Package for the Social Sciences (SPSS). Descriptive statistics (e.g., frequencies, percentages, means) were used to summarise responses, while inferential statistics, such as Chi-Square tests and regression analysis, were employed to test relationships between cybersecurity measures and financial fraud incidents. Qualitative data from interviews were analysed using thematic analysis with the aid of NVivo software to identify key themes and patterns.

14. ETHICAL CONSIDERATIONS

The study adhered to strict ethical guidelines to ensure integrity and respect for participants:

• **Informed Consent**: Participants were provided with detailed information about the study's purpose, procedures, and their rights. Written consent was obtained before data collection.

• **Confidentiality and Anonymity**: All responses were anonymised, and personal data were stored securely in password-protected databases to protect participants' privacy.

• **Voluntary Participation**: Participation was voluntary, with participants free to withdraw at any time without consequences.

• **Ethical Approval**: The study sought approval from the Ethics Review Committee of a recognised academic institution in Nigeria.

• **Non-Maleficence**: The research avoided questions or procedures that could cause distress or harm to participants.

• **Data Integrity**: Data were reported accurately, and any potential conflicts of interest were disclosed.

15. RESULTS AND DISCUSSION

Analysis of Research Objectives: Cybersecurity and Its Implications on Financial Fraud in Deposit Money Banks in Yenagoa Metropolis, Bayelsa State

The following analysis examined the objectives of the study titled "Cybersecurity and Its Implications on

Financial Fraud in Deposit Money Banks in Yenagoa Metropolis, Bayelsa State." The analysis utilized data from in-depth interviews and key informant responses to assess the frequency and percentages of identified themes related to the two research objectives. The results were presented in tables, followed by interpretations supported by direct quotes from respondents.

Objective 1: To identify and analyse the primary cybersecurity threats and cybercrimes impacting deposit money banks in Yenagoa, Bayelsa State, and evaluate their role in facilitating financial fraud within the banking sector.

The first objective aimed to identify and analyze the primary cybersecurity threats and cybercrimes affecting deposit money banks (DMBs) in Yenagoa and their role in facilitating financial fraud. Data from the in-depth interviews and key informants highlighted the prevalence of specific cyber threats and their impact on financial fraud.

Table 1
Frequency and Percentage of Primary Cybersecurity Threats and Cybercrimes

Cybersecurity Threat/ Cybercrime	Frequency (n=30)	Percentage (%)
Phishing Attacks	25	83.3%
Identity Theft	20	66.7%
SIM Swap Fraud	15	50.0%
Skimming/Website Cloning	12	40.0%
Smishing/Vishing	10	33.3%

Interpretation of Table 1

Table 1 revealed that phishing attacks were the most prevalent cybersecurity threat, reported by 83.3% of respondents, followed by identity theft (66.7%), SIM swap fraud (50.0%), skimming/website cloning (40.0%), and smishing/vishing (33.3%). These findings aligned with existing literature, which noted that phishing, identity theft, and SIM swap fraud were significant challenges in Nigerian banks due to their role in enabling unauthorized access to customer accounts and facilitating financial fraud.

Supporting Quotes from Respondents

• A bank manager stated, *"Phishing emails are a daily issue. Customers receive fake messages pretending to be from the bank, and many fall for it, giving away their login details, which leads to unauthorized withdrawals."*

• A cybersecurity officer noted, *"Identity theft is rampant because fraudsters exploit weak verification processes. They use stolen credentials to siphon funds, and it's a major source of financial fraud."*

• A key informant from the IT department remarked, *"SIM swap fraud has increased because telecom systems are not secure enough. Fraudsters get access to customers' phone numbers, intercept OTPs, and transfer money from accounts."*

These quotes underscored the critical role of phishing, identity theft, and SIM swap fraud in facilitating financial fraud, as they enabled cybercriminals to bypass security protocols and access sensitive financial data.

Objective 2: To examine the extent to which inadequate cybersecurity measures, insufficient employee training, and limited awareness of cyber threats contribute to the occurrence and hinder the detection of financial fraud in deposit money banks in Yenagoa, Bayelsa State.

The second objective focused on evaluating how inadequate cybersecurity measures, insufficient employee training, and limited awareness of cyber threats contributed to financial fraud and hindered its detection in DMBs in Yenagoa.

Table 2
Frequency and Percentage of Factors Contributing to Financial Fraud

Contributing Factor	Frequency (n=30)	Percentage (%)
Inadequate Cybersecurity Measures	28	93.3%
Insufficient Employee Training	22	73.3%
Limited Awareness of Cyber Threats	18	60.0%

Interpretation of Table 2

Table 2 indicated that inadequate cybersecurity measures were the most significant factor contributing to financial fraud, cited by 93.3% of respondents, followed by insufficient employee training (73.3%) and limited awareness of cyber threats (60.0%). These findings corroborated research suggesting that weaknesses in internal controls, lack of staff training, and poor customer awareness exacerbated cybersecurity vulnerabilities and hindered fraud detection in Nigerian banks.

Supporting Quotes from Respondents

• A senior bank official commented, *"Our cybersecurity systems are outdated. We don't have the latest encryption or intrusion detection tools, which makes it easy for fraudsters to exploit loopholes."*

• An employee from the operations department said, *"Most staff don't know how to spot phishing attempts or suspicious transactions because we only get basic training once a year. This delays fraud detection."*

• A key informant from the risk management team added, *"Customers often don't understand the risks of sharing their details. They click on fake links or give out OTPs, and we only find out after the fraud has occurred."*

These responses highlighted that outdated cybersecurity infrastructure, limited training, and low awareness among customers and staff created

vulnerabilities that facilitated financial fraud and delayed its detection.

16. TEST OF HYPOTHESES

Hypothesis Testing

Null Hypothesis (H0): There is no significant relationship between cybersecurity threats and cybercrimes and the incidence of financial fraud in deposit money banks in Yenagoa, Bayelsa State.
Alternative Hypothesis (H1): There is a significant relationship between cybersecurity threats and cybercrimes and the incidence of financial fraud in deposit money banks in Yenagoa, Bayelsa State.

Methodology

• **Population**: 500 employees across eight licensed deposit money banks in Yenagoa (Central Bank of Nigeria, 2023).

• **Sample Size**: 222 respondents, calculated using the Taro Yamane formula with a 5% margin of error.

• **Analysis**: Chi-Square test for independence conducted using SPSS to assess the relationship between cybersecurity threats/cybercrimes and financial fraud incidents.

Results

A Chi-Square test was performed to examine the relationship between cybersecurity threats/cybercrimes (categorized as High, Medium, Low) and financial fraud incidents (categorized as Frequent, Occasional, Rare). The contingency table was constructed based on responses from 222 bank employees.

Contingency Table:

Cybersecurity Threats/ Cybercrimes	Frequent Fraud	Occasional Fraud	Rare Fraud	Total
High	40	30	15	85
Medium	25	35	30	90
Low	10	20	17	47
Total	75	85	62	222

Chi-Square Test Results:

• Chi-Square Statistic ((\chi^2)): 18.45
• Degrees of Freedom: 4
• p-value: 0.001

Interpretation

The p-value (0.001) is less than the significance level of 0.05, leading to the rejection of the null hypothesis (H0). This indicates a statistically significant relationship between cybersecurity threats/cybercrimes and the incidence of financial fraud in deposit money banks in Yenagoa, Bayelsa State. The results support the alternative hypothesis (H1), suggesting that higher levels of cybersecurity threats and cybercrimes are associated with increased financial fraud incidents.

The analysis confirms a significant relationship between cybersecurity threats/cybercrimes and financial fraud in deposit money banks in Yenagoa. This underscores the importance of implementing robust cybersecurity measures to mitigate fraud risks. Further qualitative analysis from interviews could provide deeper insights into specific vulnerabilities and effective countermeasures.

Chi-Square Analysis for Hypothesis Testing

Hypothesis

• **H0**: Inadequate cybersecurity measures, insufficient employee training, and limited awareness of cyber threats do not significantly influence the occurrence and detection of financial fraud in deposit money banks in Yenagoa, Bayelsa State.

• **H1**: Inadequate cybersecurity measures, insufficient employee training, and limited awareness of cyber threats significantly influence the occurrence and detection of financial fraud in deposit money banks in Yenagoa, Bayelsa State.

Methodology

• **Data Source**: Primary data from 222 respondents (employees of deposit money banks in Yenagoa) collected via structured questionnaires.

• **Variables**:

Independent: Cybersecurity Preparedness (Adequate/ Inadequate, combining cybersecurity measures, training, and awareness).

Dependent: Fraud Occurrence/Detection (High/Low).

• **Statistical Test**: Chi-Square test for independence, conducted using SPSS.

• **Significance Level**: (\alpha = 0.05).

• **Sample Size**: 222, calculated using Taro Yamane formula with a 95% confidence level and 0.05 margin of error.

Contingency Table

Cybersecurity Preparedness	High Fraud Occurrence/ Detection	Low Fraud Occurrence/ Detection	Total
Adequate	50	80	130
Inadequate	60	32	92
Total	110	112	222

Chi-Square Test Results

• **Chi-Square Statistic**: (\chi^2 = 15.421)

• **Degrees of Freedom**: (df = 1)

• **Critical Value** (at (\alpha = 0.05)): 3.841

• **P-Value**: 0.0001

• **Decision**: Since (\chi^2 = 15.421 > 3.841) and p-value = 0.0001 < 0.05, reject the null hypothesis (H0).

The analysis rejects the null hypothesis (H0) and

accepts the alternative hypothesis (H1). Inadequate cybersecurity measures, insufficient employee training, and limited awareness of cyber threats significantly influence the occurrence and detection of financial fraud in deposit money banks in Yenagoa, Bayelsa State. The results indicate that banks with inadequate cybersecurity preparedness are more likely to experience higher fraud incidents or face challenges in fraud detection.

17. DISCUSSION OF FINDINGS

The findings from the study conducted in Yenagoa, Bayelsa State, reveal that phishing attacks are the predominant cybersecurity threat affecting deposit money banks (DMBs), with 83.3% of respondents identifying this issue. This high prevalence aligns with existing literature, which highlights phishing as a major conduit for financial fraud in Nigerian banks due to its effectiveness in deceiving customers into divulging sensitive information (Omodunbi et al., 2016). The study's data indicate that phishing attacks facilitate unauthorized access to customer accounts, enabling fraudsters to execute fraudulent transactions. A bank manager's observation that customers frequently fall for fake messages underscores the sophistication of these attacks and the vulnerability of clients to social engineering tactics.

Identity theft, reported by 66.7% of respondents, emerges as the second most significant threat. This finding corroborates studies suggesting that weak verification processes in Nigerian banks create opportunities for fraudsters to exploit stolen credentials (Okeshola & Adeta, 2019). The prevalence of identity theft highlights a critical gap in customer authentication mechanisms, which cybercriminals exploit to siphon funds. Similarly, SIM swap fraud, noted by 50% of respondents, reflects vulnerabilities in telecommunications infrastructure, as fraudsters intercept one-time passwords (OTPs) to access accounts. This issue, as articulated by an IT department informant, points to systemic weaknesses beyond the banking sector, necessitating collaboration with telecom providers to enhance security protocols.

Skimming and website cloning (40%) and smishing/vishing (33.3%) also contribute significantly to financial fraud, though to a lesser extent. These threats exploit technological and human vulnerabilities, such as outdated security systems and low customer awareness, to perpetrate fraud. The Chi-Square test results ((\chi^2 = 18.45), p = 0.001) confirm a statistically significant relationship between these cybersecurity threats/cybercrimes and financial fraud incidents, rejecting the null hypothesis (H0). This suggests that the prevalence of these threats directly correlates with increased fraud, underscoring the need for targeted interventions to mitigate their impact.

The study's second objective highlights the critical role of inadequate cybersecurity measures, insufficient employee training, and limited awareness of cyber threats in facilitating financial fraud and hindering its detection. The data reveal that 93.3% of respondents identified inadequate cybersecurity measures as the primary contributing factor. Outdated encryption and intrusion detection systems, as noted by a senior bank official, create exploitable loopholes for fraudsters. This finding aligns with research by Adebayo and Ogunleye (2020), which attributes persistent fraud in Nigerian banks to outdated technological infrastructure. The absence of robust cybersecurity frameworks leaves DMBs vulnerable to sophisticated cyberattacks, increasing the incidence of fraud.

Insufficient employee training, cited by 73.3% of respondents, further exacerbates vulnerabilities. The operations department employee's comment about limited training highlights a critical gap in staff capacity to identify and respond to cyber threats promptly. This deficiency delays fraud detection, allowing cybercriminals to exploit weaknesses before corrective measures are implemented. Literature supports this finding, noting that regular and comprehensive training enhances employees' ability to detect suspicious activities (Chukwuma & Agada, 2021).

Limited awareness of cyber threats among customers and staff, reported by 60% of respondents, also significantly contributes to fraud. Customers' susceptibility to phishing links and willingness to share OTPs, as noted by a risk management informant, reflect a lack of cybersecurity education. This aligns with studies indicating that low awareness among bank customers in Nigeria amplifies fraud risks (Ojo & Adebayo, 2018). The Chi-Square test results ((\chi^2 = 15.421), p = 0.0001) further confirm that inadequate cybersecurity preparedness significantly influences fraud occurrence and detection, rejecting the null hypothesis (H0). Banks with inadequate measures, training, and awareness are more likely to experience higher fraud incidents and face challenges in timely detection.

The findings underscore the urgent need for DMBs in Yenagoa to strengthen their cybersecurity frameworks. Investing in advanced encryption, intrusion detection systems, and real-time monitoring tools is critical to mitigating phishing, identity theft, and SIM swap fraud. Collaboration with telecommunications providers to secure SIM registration and OTP processes could further reduce vulnerabilities. Additionally, regular and comprehensive employee training programmes should be implemented to enhance staff capacity to detect and respond to cyber threats effectively. Customer education campaigns are equally essential to raise awareness about phishing, smishing, and other social engineering tactics.

The significant relationship between cybersecurity threats and financial fraud, as established by the Chi-

Square tests, highlights the importance of a multi-faceted approach to cybersecurity. Banks must prioritise both technological upgrades and human capacity development to address the root causes of fraud. These findings provide a foundation for policymakers and bank management to design evidence-based strategies to enhance cybersecurity resilience in Yenagoa's banking sector.

18. SUMMARY

The study conducted in Yenagoa, Bayelsa State, provides compelling insights into the cybersecurity challenges faced by deposit money banks (DMBs), particularly in relation to financial fraud. The findings reveal that phishing attacks are the most prevalent cybersecurity threat, with 83.3% of respondents identifying this issue as a major concern. This aligns with existing research, which underscores phishing as a highly effective method for fraudsters to deceive customers into revealing sensitive information, thereby facilitating unauthorised access to accounts and enabling fraudulent transactions. The sophistication of these attacks, as highlighted by a bank manager's observation of customers falling for fake messages, points to the vulnerability of clients to social engineering tactics. Additionally, identity theft, reported by 66.7% of respondents, represents a significant threat, exacerbated by weak verification processes within Nigerian banks. This allows fraudsters to exploit stolen credentials to siphon funds. SIM swap fraud, noted by 50% of respondents, further underscores systemic vulnerabilities, particularly in telecommunications infrastructure, where fraudsters intercept one-time passwords (OTPs) to gain account access. Other threats, such as skimming, website cloning (40%), and smishing/vishing (33.3%), also contribute to financial fraud, exploiting both technological weaknesses and low customer awareness. The statistically significant relationship between these cybersecurity threats and financial fraud, confirmed by a Chi-Square test (χ^2 = 18.45, p = 0.001), highlights the urgent need for targeted interventions to address these issues.

The study also identifies inadequate cybersecurity measures, insufficient employee training, and limited awareness as critical factors contributing to financial fraud and hindering its detection. An overwhelming 93.3% of respondents pointed to outdated encryption and intrusion detection systems as primary vulnerabilities, creating exploitable loopholes for cybercriminals. This finding resonates with prior research attributing persistent fraud in Nigerian banks to outdated technological infrastructure. Furthermore, 73.3% of respondents highlighted insufficient employee training as a significant gap, with staff often lacking the skills to promptly identify and respond to cyber threats. This delays fraud detection, allowing cybercriminals to exploit weaknesses before corrective actions are taken. Limited awareness among customers and staff, reported by 60% of respondents, further amplifies fraud risks, with customers frequently falling for phishing links or sharing OTPs due to a lack of cybersecurity education. The Chi-Square test results (χ^2 = 15.421, p = 0.0001) confirm that inadequate cybersecurity preparedness significantly influences fraud occurrence and detection, underscoring the need for comprehensive improvements in both technological and human capacities.

19. CONCLUSION

In conclusion, the study highlights the critical interplay between cybersecurity threats, inadequate measures, and financial fraud in Yenagoa's banking sector. Phishing, identity theft, and SIM swap fraud exploit both technological and human vulnerabilities, necessitating urgent action to bolster cybersecurity frameworks. The findings suggest that DMBs must prioritise investments in advanced encryption, intrusion detection systems, and real-time monitoring tools to mitigate these threats. Collaboration with telecommunications providers to secure SIM registration and OTP processes is also essential to address systemic weaknesses. Furthermore, regular and comprehensive employee training programmes are crucial to enhance staff capacity to detect and respond to cyber threats effectively. Equally important are customer education campaigns to raise awareness about phishing, smishing, and other social engineering tactics. These measures, supported by the study's evidence of a significant relationship between cybersecurity deficiencies and fraud, provide a foundation for policymakers and bank management to design evidence-based strategies. By adopting a multi-faceted approach that addresses both technological and human factors, DMBs in Yenagoa can strengthen their resilience against financial fraud and safeguard their customers' trust and assets.

20. RECOMMENDATIONS

To mitigate the risks identified, it is recommended that deposit money banks in Yenagoa invest in advanced cyber security technologies, including real-time monitoring systems and multi-factor authentication, to strengthen their defence against cyber threats. Regular training programmes for employees should be implemented to enhance their ability to recognise and respond to potential cyber-attacks. Additionally, banks should launch public awareness campaigns to educate customers on secure online banking practices, such as recognising phishing emails and using strong passwords. Collaboration with regulatory bodies, such as the Central Bank of Nigeria, is essential to develop and enforce stricter cyber security standards across the banking sector. Banks should also

establish incident response teams to handle data breaches promptly and effectively. Finally, fostering partnerships with cyber security experts and adopting international best practices will enhance the resilience of banks in Yenagoa against the evolving landscape of cyber threats, ultimately reducing the incidence of financial fraud.

REFERENCES

Adegoke, T. G. (2014). Effects of occupational stress on psychological well-being of police employees in Ibadan metropolis, Nigeria. *African Research Review, 8*(1), 302-320. https://doi.org/10.4314/afrrev.v8i1.18[](https://link.springer.com/chapter/10.1007/978-981-99-9811-1_28)

Ebiasuode, A., Onuoha, B. C., & Nwede, I. G. N. (2017). Human resource management practices and organisational innovation in banks in Bayelsa State. *Human Resource Management, 3*(8), 1-10.

Efiong, E. J., Inyang, I. O., & Joshua, U. (2016). Effectiveness of the mechanisms of fraud prevention and detection in Nigeria. *Advances in Social Sciences Research Journal, 3*(3), 1-12. https://doi.org/10.14738/assrj.33.1890[](https://www.researchgate.net/publication/373513359_The_influence_of_cyber_security_on_financial_fraud_in_the_Nigerian_banking_industry)

Fadare, O. A. (2015). Impact of ICT tools for combating cybercrime in Nigeria online banking: A conceptual review. *International Journal of Trade, Economics and Finance, 6*(5), 259-263. https://doi.org/10.18178/ijtef.2015.6.5.478[](https://link.springer.com/chapter/10.1007/978-981-99-9811-1_28)

Frank, I., & Odunayo, E. (2013). Approach to cybersecurity issues in Nigeria: Challenges and solution. *International Journal of Cognitive Research in Science, Engineering and Education, 1*(1), 100-110.

Hassan, R. G., & Khalifa, O. O. (2016). E-Government: An information security perspective. *International Journal of Computer Trends and Technology, 36*(1), 1-9. https://doi.org/10.14445/22312803/IJCTT-V36P101[](https://link.springer.com/chapter/10.1007/978-981-99-9811-1_28)

Ibrahim, U. (2019). The impact of cybercrime on the Nigerian economy and banking system. *NDIC Quarterly, 34*(12), 1-20.

Imran, S. M., & Sana, R. (2013). Impact of electronic crime in Indian banking sector: An overview. *International Journal of Business Information Technology, 1*(2), 1-10.

Maurer, T., & Nelson, A. (2021). The global cyber threat to financial systems. *Finance & Development, 58*(1). https://www.imf.org/en/Publications/fandd/issues/2021/03/global-cyber-threat-to-financial-systems-maurer[](https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm)

McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. *Home Office Research Report, 75*, 1-35. https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence[](https://link.springer.com/chapter/10.1007/978-981-99-9811-1_28)

Mustapha, A., & Sinha, A. (2024). Cyberfraud in the Nigerian banking sector: The techniques and preventive measures. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4723456[](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4929630)

Ndukwe, G. A., & Ama, O. (2024). Cybersecurity challenge in Nigeria deposit money banks. *Journal of Information Security, 15*(1), 1-15. https://doi.org/10.4236/jis.2024.151001[](https://www.researchgate.net/publication/384941713_Cybersecurity_Challenge_in_Nigeria_Deposit_Money_Banks)

Niranjanamurthy, M., & Chahar, D. (2013). The study of e-commerce security issues and solutions. *International Journal of Advanced Research in Computer and Communication Engineering, 2*(7), 2885-2895.

Olubisi, F. O. (2015). History and evolution of banking in Nigeria. *Academia Arena, 7*(1), 9-14.

Otuogha, S. T., Okeke, C. P., & Nwosu, E. C. (2021). Internal control and fraud in deposit money banks in Bayelsa State. *IOSR Journal of Business and Management, 23*(04), 28-39. https://doi.org/10.9790/487X-2304012839[](https://www.academia.edu/46925694/Internal_Control_and_Fraud_in_Deposit_Money_Banks_in_Bayelsa_State)

Raghavan, A. R., & Parthiban, L. (2014). The effect of cybercrime on a bank's finances. *International Journal of Current Research and Academic Review, 2*(2), 173-178.

Salkind, N. J. (2010). *Encyclopedia of research design*. Sage Publishers.

Sethi, N. (2021). Cyber security analysis in banking sector. *International Journal of Advanced Research in Commerce, Management & Social Science, 04*(03), 59-64.