GAS Journal of Engineering and Technology (GASJET)

Volume 2, Issue 5, 2025 Journal Homepage: https://gaspublishers.com/gasjet-home/ ISSN: 3048-5800
Email: editor@gaspublishers.com

Ensuring a Secure Future by Insuring Against Cybercrime: A Study of Okada Micro Finance Bank, Okada, Edo State

Omorogbe Osasu Harry (Phd)[1]; Obande, Bonnie Obeka (CLN)[2]; Amoforitse, Fortune Ighotuweyin[3]; Eduje, Anthony Ighoakpo[4] & Omoregie Dolly Arenvbaguehita[5]

[1]Department of Cyber Security, Igbinedion University, Okada. Edo State, Nigeria.
[2]Igbinedion University Library, Okada, Edo State, Nigeria.
[3]Department of Cyber Security and ICT Unit, Igbinedion University, Okada. Edo State, Nigeria.
[4]Greenwich Holdings Limited Victoria Island, Lagos.
[5]Harresearchwork: Igbinedion University Okada.

Received: 19.07.2025 | **Accepted:** 30.07.2025 | **Published:** 13.08.2025

***Corresponding Author:** Obande, Bonnie Obeka

DOI: *10.5281/zenodo.16846656*

Abstract **Original Research Article**

Cybercrime poses an increasing threat to financial institutions worldwide, with microfinance banks in developing countries like Nigeria being particularly vulnerable due to limited cybersecurity infrastructure. This study investigates how Okada Micro Finance Bank can ensure a secure future by insuring against cybercrime through the adoption of cyber insurance and enhanced cyber risk management practices. Using a mixed-method approach, data were collected from staff and IT personnel to evaluate the bank's exposure to cyber threats, existing security measures, and the level of awareness and adoption of cyber insurance. Findings reveal a high exposure to cyber threats, limited cybersecurity practices, and minimal awareness or use of cyber insurance. The study concludes that while cyber insurance remains an underutilized tool, it holds significant potential in strengthening the resilience of microfinance institutions. Recommendations include the adoption of tailored cyber insurance policies, increased staff training, regulatory support, and public-private partnerships to enhance cybersecurity preparedness. This research contributes to the discourse on digital risk management and financial security in Nigeria's microfinance sector.

Keywords: Cybercrime, Cyber Insurance, Microfinance, Risk Management, Financial Security.

INTRODUCTION

In today's digital financial ecosystem, cybercrime presents one of the most significant threats to financial institutions, especially microfinance banks that often operate with limited cybersecurity infrastructure. As Nigeria's digital economy continues to grow, institutions like Okada Micro Finance Bank (MFB) are increasingly exposed to cyber risks ranging from phishing attacks to ransomware and unauthorized access to customer data. Consequently, the idea of cyber insurance is gaining traction as a strategic risk mitigation approach. This study explores how Okada MFB can ensure a secure future by adopting cyber insurance and other cyber risk management practices to combat rising cyber threats.

LITERATURE REVIEW

The Rise of Cybercrime in the Financial Sector

Cybercrime has emerged as a significant global threat to financial systems, particularly with the rapid digitization of banking services. Financial institutions are attractive targets due to the vast amount of sensitive customer data and financial transactions they process (Kshetri, 2019). In Nigeria, cybercrime has evolved from simple scams to more complex attacks involving malware, phishing, ransomware, and insider threats (Okeshola & Adeta, 2013). Microfinance banks, often perceived as less fortified than commercial banks, are particularly vulnerable because they lack the financial and

technical capacity to implement comprehensive cyber security systems (Akinyemi & Adegbola, 2022).

Impact of Cybercrime on Microfinance Institutions

The consequences of cyber-attacks on microfinance institutions can be devastating, ranging from financial losses and reputational damage to legal liabilities and erosion of customer trust. For smaller institutions like Okada Micro Finance Bank, even a single breach can threaten operational continuity. According to Adewoye (2020), Nigerian microfinance banks report losses running into millions of naira due to security breaches annually, yet many continue to operate without standardized risk management protocols. The nature of services provided by microfinance banks—often involving rural and low-income clients—further amplifies the need for resilient and secure operations.

Cyber Insurance: A Strategic Risk Mitigation Tool

Cyber insurance has emerged globally as a strategic approach to managing cyber risk. It involves the transfer of risk through financial products that provide coverage for data breaches, network damage, legal liabilities, and business interruption (Romanosky et al., 2019). In developed countries, cyber insurance is becoming a standard component of enterprise risk management. However, in Nigeria, the adoption is still in its infancy. Adebayo and Alhassan (2021) found that less than 10% of financial institutions in Nigeria have active cyber insurance policies, largely due to a lack of awareness, inadequate regulatory frameworks, and mistrust in insurance companies.

Barriers to Cyber Insurance Adoption in Nigeria

Several challenges hinder the widespread adoption of cyber insurance in the Nigerian financial sector. These include a lack of cyber risk awareness among executives, underdeveloped insurance markets, insufficient legal frameworks for cyber liability, and limited actuarial data to assess premiums (Onifade & Oyeniran, 2022). Moreover, many microfinance banks do not perceive themselves as targets, which leads to complacency in implementing cyber risk strategies. Regulatory bodies such as the Central Bank of Nigeria have only recently begun to develop cybersecurity guidelines for microfinance institutions, indicating a policy gap that needs urgent attention (CBN, 2023).

Theoretical Perspective: Risk Management and Information Security Frameworks

From a theoretical standpoint, the study is underpinned by enterprise risk management theory and information security management frameworks. According to ISO/IEC 27001, organizations must adopt a systematic approach to managing sensitive data, including people, processes, and IT systems. Risk management models such as COSO (Committee of Sponsoring Organizations of the Treadway Commission) provide a structure for identifying, assessing, and responding to risks. Cyber insurance is considered a key risk response strategy—specifically, a transfer mechanism—when internal controls are insufficient.

Empirical Studies on Cybersecurity and Insurance in Nigeria

Empirical studies on cybersecurity and cyber insurance in Nigeria are limited but growing. Olayemi (2014) studied cybercrime impacts on Nigerian banks and found a positive correlation between digital adoption and cyber threats. Meanwhile, a more recent study by Ekezie and Ukaegbu (2023) explored cyber risk perception in Nigerian financial institutions and emphasized the urgent need for capacity building and policy enforcement. These findings align with the growing body of research that calls for cyber insurance as a complementary tool to cybersecurity technologies.

STATEMENT OF THE PROBLEM

The increasing integration of digital technologies in the financial sector has brought immense benefits in terms of efficiency, accessibility, and scalability. However, this digital transformation has also introduced significant vulnerabilities, particularly in the form of cybercrime. In Nigeria, cybercrime is on the rise, targeting both large financial institutions and smaller entities such as microfinance banks. Okada Micro Finance Bank, like many others in the sector, faces growing risks associated with phishing, ransom ware, identity theft, and unauthorized data access.

Despite these threats, many microfinance institutions lack robust cybersecurity frameworks and do not invest adequately in cyber insurance or risk mitigation strategies. There is a prevailing gap in awareness, preparedness, and response mechanisms to combat the increasingly sophisticated tactics of cybercriminals. Additionally, regulatory and infrastructural challenges further limit the ability of microfinance banks to adopt proactive security measures.

This study seeks to investigate the extent to which Okada Micro Finance Bank is exposed to cyber threats and to assess whether cyber insurance can serve as a viable strategy to safeguard its operations. It also explores the challenges hindering the adoption of such protective measures and aims to propose actionable solutions for ensuring a more secure and resilient financial future.

Research Objectives

1. To assess the level of exposure of Okada Micro Finance Bank to cybercrime.
2. To evaluate existing cybersecurity measures in place at Okada MFB.
3. To examine the awareness and adoption of cyber insurance in Okada MFB.
4. To identify the challenges and prospects of insuring against cybercrime in microfinance banks.

Research Questions

1. What types of cyber threats does Okada MFB face?
2. What cybersecurity policies and practices are currently in place?
3. To what extent is Okada MFB aware of and adopting cyber insurance?
4. What are the challenges hindering the adoption of cyber insurance?

Enterprise Risk Management (ERM) Theory

Overview of ERM Theory:

Enterprise Risk Management (ERM) refers to the process by which organizations identify, assess, manage, and monitor risks that could affect the achievement of strategic objectives. The **COSO ERM Framework** (developed by the Committee of Sponsoring Organizations of the Treadway Commission) is the most widely used ERM model.

- It includes components such as **risk identification, risk analysis, risk response (accept, mitigate, transfer, avoid)**, and risk monitoring.
- **Risk transfer**, such as through **insurance**, is a core principle of ERM.

METHODOLOGY

The study was conducted at **Okada Microfinance Bank** in Okada, Edo State, Nigeria, focusing on understanding cybercrime risks and the role of cyber insurance in mitigating them.

The **population** consisted of **10 key staff members**, including the Managing Director, Head of ICT, Head of Operations, Head of Credit, Internal Auditor, and other top management officials directly involved in ICT, risk, and compliance.

A **purposive sampling technique** was used to select participants based on their roles and relevance to the subject matter.

Data collection was carried out through:

- **Structured interviews** with top management, and
- **Questionnaires** for other selected staff.

Data analysis involved:

- **Descriptive statistics** (e.g., frequencies and percentages) for questionnaire data.
- **Thematic analysis** for interview responses.

DATA ANALYSIS AND INTERPRETATION

Population: 10 Key Staff (MD, Head of ICT, Head of Operations, Head of Credit, Internal Auditor, Compliance Officer, Risk Officer, etc.)

Objective 1: To assess the level of exposure of Okada Microfinance Bank to cybercrime

Exposure to Cybercrime Frequency Percentage

High	4	40%
Moderate	5	50%
Low	1	10%

Table 1: Approximately **50% of respondents** rated the exposure of Okada Microfinance Bank (MFB) to cybercrime as *moderate*, while **40% perceived it as *high***. This reflects a growing concern about cybersecurity threats among key personnel. Such perceptions align with the increasing **vulnerability of financial institutions to digital threats**, especially as they adopt more ICT-based operations without proportionate investment in security infrastructure (Adeniran & Osunade, 2021; Adewoye, 2020; Eze & Agbo, 2023). The results suggest that despite technological progress, microfinance institutions like Okada MFB may be underprepared to withstand sophisticated cyberattacks.

Objective 2: To evaluate existing cyber security measures in place at Okada MFB

Cyber security Measures Implemented

	Yes	No
Antivirus/Firewall Protection	10	0
Staff Cybersecurity Training	4	6
Regular Cybersecurity Audits	3	7
Two-Factor Authentication (2FA)	6	6
Cybersecurity Policy Document	5	5

Table 2: While basic cybersecurity measures such as antivirus software and firewalls are implemented across most institutions (100%), only 40% of staff receive regular cybersecurity training and just 30% report that periodic audits are conducted. This discrepancy significantly increases organizational risk exposure, as **human error continues to be a major contributing factor to cybersecurity breaches** (Adewoye, 2020; Kshetri, 2019). Research consistently shows that while technological safeguards are crucial, the absence of continuous training and oversight undermines their effectiveness, especially in sectors like microfinance banking where digital literacy levels among staff vary (Eze & Agbo, 2023).

Objective 3: To examine the awareness and adoption of cyber insurance in Okada MFB

Cyber Insurance Awareness and Adoption Frequency Percentage

Aware and Adopted	1	10%
Aware but Not Adopted	5	50%
Not Aware	4	40%

Table 3: Only 10% of the respondents indicate that cyber insurance has been adopted. While Table 3 above: Shows that 50% of respondents are aware of the existence of cyber insurance, they have not taken any steps to adopt or implement it. This indicates a significant gap between awareness and action, which may be attributed to a lack of in-depth understanding, low perceived urgency, or inadequate prioritization of cyber insurance as a critical risk management strategy (Adebayo & Alhassan, 2021; Onifade & Oyeniran, 2022; Okafor & Uzochukwu, 2021). Research has shown that awareness alone does not guarantee adoption, especially in institutions where cyber threats are underestimated or budgets are limited (Romanosky et al., 2019)

Objective 4: To identify the challenges and prospects of insuring against cybercrime in microfinance banks

Identified Challenges	Frequency
High Cost of Premiums	7
Lack of Awareness	6
Complexity in Policy Terms	5
Perceived Low Risk by Management	4
Limited Local Insurance Providers for Cyber Risks	6

Table 4 Above: Show that the major challenges facing the adoption of cyber insurance in microfinance banks such as Okada MFB include high premium costs (70%)**,** limited awareness among decision-makers (60%)**,** and the absence of clear, user-friendly insurance policies**.** Furthermore, management's perception of cyber risks as minimal significantly reduces the perceived need for such coverage**,** thereby diminishing demand (Adebayo & Alhassan, 2021; Ekezie & Ukaegbu, 2023; Onifade & Oyeniran, 2022). These factors collectively hinder the widespread uptake of cyber insurance not only in Okada MFB but across Nigeria's microfinance sector, where financial and technological literacy levels often vary.

DISCUSSION OF FINDINGS

The findings reveal that Okada Microfinance Bank faces moderate to high cyber risk exposure, especially as it increasingly adopts digital platforms. While some cyber security measures are in place, gaps in training and audits leave the bank vulnerable.

The adoption of cyber insurance is extremely low, largely due to lack of awareness, cost concerns, and the complexity of available policies. Most staff acknowledge the benefits of such insurance but cite institutional and market-level barriers to adoption.

This implies a need for regulatory bodies and the bank's management to intensify cyber security education and promote partnerships with local insurance firms to design tailored, affordable cyber insurance products for microfinance banks.

CONCLUSION

Cybercrime poses a significant threat to the sustainability and security of microfinance banks in Nigeria. While Okada MFB

has taken some measures to protect its systems, the absence of cyber insurance leaves it financially vulnerable. Awareness and education on cyber insurance must be intensified, and policy efforts should support its integration into broader cybersecurity strategies.

RECOMMENDATIONS

1. **Cyber Insurance Adoption:** Okada MFB should explore affordable cyber insurance plans tailored to the needs of microfinance institutions.
2. **Policy Development:** Regulators like the CBN should mandate minimum cyber risk coverage for all financial institutions.
3. **Capacity Building:** Regular staff training and system audits should be conducted to enhance cyber preparedness.

Public-Private Partnerships: Engage with cyber insurance firms and IT companies for better risk assessment and solutions.

REFERENCES

Adebayo, O., & Alhassan, M. (2021). Cyber insurance adoption among Nigerian financial institutions: Awareness, challenges, and prospects. *African Journal of Information Security, 9*(1), 34–48.

Adeniran, T., & Osunade, O. (2021). Cybersecurity threats and banking operations in Nigeria. *Journal of Digital Security, 13*(2), 134–145.

Adewoye, J. O. (2020). Cybersecurity awareness and preparedness of microfinance banks in Nigeria. *Journal of Financial Risk and Compliance, 7*(2), 15–28.

Akinyemi, F. T., & Adegbola, E. A. (2022). Cyber threats and financial inclusion in Nigeria: The role of microfinance banks. *African Banking Review, 11*(4), 112–129.

Central Bank of Nigeria. (2023). *Guidelines for cybersecurity in financial institutions*. CBN Publications.

Ekezie, C. M., & Ukaegbu, F. (2023). Cyber risk perception and insurance readiness among Nigerian banks. *International Journal of Cybersecurity Studies, 3*(1), 55–70.

Eze, C., & Agbo, F. (2023). Cyber risk management in Nigeria's microfinance sector. *African Journal of Information Systems, 7*(1), 45–60.

Kshetri, N. (2019). Cybersecurity management in the financial sector: Global threats and local responses. *Journal of Financial Crime, 26*(2), 421–435.

Ojo, O., & Akinwale, A. (2020). Cyber insurance as a financial safeguard for Nigerian banks. *Journal of Financial Risk Management, 5*(4), 211–225.

Okafor, I., & Uzochukwu, C. (2021). The role of cyber insurance in restoring consumer trust after cyber incidents. *Journal of Information Policy, 9*(3), 289–304.

Okeshola, F. B., & Adeta, A. K. (2013). The nature, causes and consequences of cyber crime in tertiary institutions in Zaria, Kaduna State, Nigeria. *American International Journal of Contemporary Research, 3*(9), 98–114.

Okoye, M., & Onuoha, N. (2022). The rise of cybercrime in Nigeria: Implications for financial services. *Nigerian Journal of Cyber Policy, 4*(2), 75–89.

Olayemi, O. (2014). A socio-technological analysis of cybercrime and cybersecurity in Nigeria. *International Journal of Sociology and Anthropology, 6*(3), 116–125.

Onifade, T. A., & Oyeniran, A. T. (2022). Cyber insurance: A necessary risk mitigation strategy for Nigerian enterprises. *Journal of Insurance and Risk Management, 5*(2), 63–79.

Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cybersecurity, 5*(1), 1–18.