ACU Journal of Social Sciences
https://ajss.acu.edu.ng

Cyber Risks and the Nigerian Business Sector: A Critical Analysis of the Emerging Cyber Insurance Market in Nigeria

Amos Ayodeji OGUNYEMI
University of the West of Scotland
amos.ogunyemi@yahoo.com

Abstract

This study explores the impact of cyber risk exposure on the financial security, operational continuity, profitability, and demand for cyber insurance among Nigerian businesses, drawing on data from 250 respondents. Employing a mixed-methods research design, the study integrates descriptive analysis, correlation, and regression techniques to provide a comprehensive examination of the subject. The research reveals that heightened cyber risk exposure significantly undermines the financial security and operational continuity of businesses, with a notable negative effect on profitability. A positive correlation between business size and demand for cyber insurance was identified, suggesting that larger businesses are more inclined to invest in such insurance. Additionally, the study finds a significant performance difference between businesses that invest in cyber insurance and those that do not, indicating the value of insurance in improving business outcomes. The study concludes with recommendations for Nigerian businesses to enhance their cybersecurity measures and invest in cyber insurance to mitigate risks and safeguard financial stability, while urging policymakers to develop supportive regulatory frameworks.

Keywords: *Cyber risk exposure, financial security, cyber insurance, profitability, operational continuity*

Introduction

In today's rapidly evolving technological landscape, Nigerian businesses are increasingly exposed to a range of cyber threats due to their growing reliance on digital platforms and interconnected systems. The rise of cybercrime has introduced significant risks such as data breaches, ransomware attacks, and phishing schemes, which challenge the confidentiality, integrity, and availability of critical information systems (Choudhary et al, 2022; George et al, 2024). These threats can lead to substantial financial losses, reputational damage, and operational disruptions (Ibiyemi & Olutimehin , 2024; Thakur, 2024; Onunka et al, 2023). As businesses seek ways to mitigate these risks, cyber insurance has emerged as a crucial tool. Cyber insurance provides financial protection and support, covering incident response, data breach notifications, legal compliance, and other costs associated with cyber incidents. However, in Nigeria, the uptake of cyber insurance remains low due to limited awareness, high costs, and inadequate knowledge about available products tailored to local businesses (Udo et al, 2024; Akintoye et al, 2022).

Cyber risks are inherent in the digital environment and include threats such as data breaches, malware attacks, and ransomware, all of which jeopardize digital assets and business operations (Olaiya et al, 2024). The global rise in cyber-attacks, exacerbated by the COVID-19 pandemic, underscores the urgent need for robust cybersecurity measures. Ransomware attacks and data breaches, in particular, have become prevalent, imposing significant financial and operational burdens on organizations (Albustanji, 2024; Temara, 2024). To combat these threats, national and international policies have been implemented, such as the GDPR and CCPA, which aim to enhance cybersecurity and protect sensitive data through comprehensive frameworks and regulations. These measures focus on critical infrastructure protection, public-private partnerships, and international cooperation, but their implementation varies across regions and sectors.

In Nigeria, despite the increasing awareness of cyber threats globally, many businesses still underestimate their vulnerability and the importance of cyber insurance. Limited awareness, high costs, and insufficient knowledge about tailored insurance options contribute to the low adoption rates of cyber insurance (Ebekozien,et al, 2023; Kineber et al., 2023). Nigerian businesses, particularly smaller enterprises, often perceive

themselves as less likely targets for cyber attacks or believe their existing security measures are adequate. This lack of recognition regarding the evolving threat landscape and the potential impact of cyber incidents on their growth and success results in a significant gap in the adoption of necessary risk mitigation strategies. As a result, Nigerian businesses need to enhance their understanding of cyber risks and the benefits of cyber insurance to better protect themselves and improve their overall cybersecurity posture.

Despite numerous studies investigating the relationship between cyber risk exposure and various business outcomes, the literature remains inconclusive, with mixed results regarding the nature and extent of this relationship. While some studies suggest a significant impact of cyber risks on financial stability and operational performance, others present conflicting findings, highlighting the complexity and variability of cyber risk management outcomes. This inconsistency prompts the question what factors contribute to the divergent findings in existing research, and how can a more cohesive understanding of the relationship between cyber risk exposure and business performance be achieved? Hence, the objective of this study is to investigate the impact of cyber risk exposure on the financial security and operational continuity of Nigerian businesses.

Research Questions

i. Is there a significant relationship between the level of cyber risk exposure and the demand for cyber insurance among Nigerian businesses?
ii. How does the size of a Nigerian business influence its willingness to invest in cyber insurance as a risk management strategy?
iii. Does the number of previous cyber attacks experienced by Nigerian businesses predict their likelihood of purchasing cyber insurance coverage?
iv. To what extent do cyber risks impact the profitability of Nigerian businesses?

Research Objectives

i. To determine if there is a significant relationship between the level of cyber risk exposure and the demand for cyber insurance among Nigerian businesses.
ii. To examine how the size of a Nigerian business influences its willingness to invest in cyber

insurance as a risk management strategy.

iii. To assess whether the number of previous cyber attacks experienced by Nigerian businesses predicts their likelihood of purchasing cyber insurance coverage.

iv. To evaluate the extent to which cyber risks impact the profitability of Nigerian businesses.

Research Hypotheses

H_{01}: There is no significant relationship between the level of cyber risk exposure and the demand for cyber insurance among Nigerian businesses.

H_{02}: The size of a Nigerian business does not significantly influence its willingness to invest in cyber insurance as a risk management strategy.

H_{03}: The number of previous cyber-attacks experienced by Nigerian businesses does not significantly predict their likelihood of purchasing cyber insurance coverage.

H_{04}: Cyber risks do not significantly impact the profitability of Nigerian businesses.

Literature Review

Cyber Risk

Cyber risks refer to the potential threats and vulnerabilities that organizations face in the digital realm, where unauthorized access, malicious attacks, and system failures can compromise the confidentiality, integrity, and availability of information systems (Strupczewski, 2021; Pugnetti et al, 2024). These risks include a wide range of cyber threats, such as data breaches, ransomware attacks, phishing scams, and denial-of-service (DoS) attacks, which can disrupt business operations, lead to significant financial losses, and damage a company's reputation. In the Nigerian business context, cyber risks are increasingly prevalent due to the rapid adoption of digital technologies and the growing sophistication of cybercriminals (Okoru & Oluku, 2024). According to Kanu et al (2024), the impact of these risks is amplified by the challenges of inadequate cybersecurity infrastructure, low levels of cyber awareness, and the evolving nature of cyber threats, making effective risk management and mitigation strategies essential for business continuity.

Cyber risks can take different forms that involve various types of threats and vulnerabilities. These include data breaches,

where unauthorized access exposes sensitive information; ransomware attacks, in which malicious software encrypts data and demands a ransom for its release; phishing scams, deceptive attempts to steal personal or financial information by impersonating a trustworthy source; and denial-of-service (DoS) attacks, which overwhelm a network with traffic to disrupt operations. Additionally, insider threats arise from within the organization, where employees or other insiders misuse their access, either maliciously or unintentionally. Other forms include advanced persistent threats (APTs), prolonged and targeted intrusions that often remain undetected, and malware, malicious software designed to damage or exploit systems. Also, social engineering involves manipulative tactics that trick individuals into revealing confidential information or granting unauthorized access. These various forms of cyber risks pose significant challenges to the security and stability of organizations (Hassan et al, 2024; Alabi et al, 2023)

Cyber Insurance

Cyber insurance is a specialized form of insurance designed to help organizations mitigate the financial impact of cyber risks, including data breaches, cyberattacks, and other digital threats (Kayode-Ajala, 2023; Wang et al, 2020). It provides coverage for a range of expenses that may arise from such incidents, including costs related to data restoration, legal fees, regulatory fines, and business interruption. Additionally, cyber insurance may cover liabilities stemming from the exposure of sensitive customer information and the costs associated with managing the reputational damage that can follow a cyber incident (Meshram & Singh, 2024; Schwieger & Ladwig, 2022). As businesses increasingly rely on digital technologies, cyber insurance has become an essential tool in managing the growing risks associated with cyber threats, providing both financial protection and support in navigating the complex landscape of cyber risk management (Cortez & Dekker, 2022**;** AL-Hawamleh, 2024)

Theoretical Framework

The theoretical framework used in this study is the Protection Motivation Theory, which was propounded by R.W. Rogers in 1975. PMT was originally developed to explain how individuals are motivated to adopt protective behaviors in the face of perceived threats, particularly in health-related contexts. The theory suggests that when confronted with a threat, individuals undergo a cognitive appraisal process involving four key components: perceived severity of the

threat, perceived vulnerability to the threat, perceived efficacy of the recommended protective behavior, and perceived self-efficacy in executing the protective behavior. This appraisal process leads to the formation of a protection motivation, which drives the individual to take action to mitigate or avoid the threat. Over time, PMT has been extended beyond health to other areas such as environmental protection, disaster preparedness, and, importantly, cybersecurity, providing a robust framework for understanding how both individuals and organizations respond to a wide range of risks (Arenas et al, 2024; Khan et al, 2023).

In relation to cyber risks and the emerging cyber insurance market in Nigeria, PMT is highly applicable as it helps explain how Nigerian businesses perceive and respond to cyber threats. The theory can be used to analyze the cognitive processes that influence a business's decision to adopt cyber insurance as a protective measure against cyber risks. Specifically, PMT helps in understanding how businesses assess the severity and likelihood of cyber threats, the perceived effectiveness of cyber insurance in mitigating these risks, and their confidence in implementing such insurance measures. For instance, studies like Bekkers et al (2024); Arenas et al (2024); also Ezati Rad et al (2021) have applied PMT to explore cybersecurity behaviors within organizations, demonstrating how perceived threats and self-efficacy drive the adoption of protective actions like cyber insurance. The strength of PMT lies in its ability to capture the psychological and behavioral factors that influence protective behaviors, making it a valuable tool for analyzing the motivations behind the adoption of cyber insurance in the Nigerian business sector. This framework provides critical perceptions into both the drivers and barriers to cyber insurance adoption, contributing to the broader understanding of cybersecurity management in emerging markets.

Empirical Review

Reis et al. (2024) investigated the cybersecurity dynamics within the Nigerian banking sector, providing an in-depth review of recent trends and strategic approaches to emerging challenges. The paper synthesizes existing literature, reports, and case studies to offer a comprehensive understanding of the current cybersecurity landscape in Nigerian banks. It focuses on identifying predominant cyber threats, such as phishing, ransomware, and insider attacks, and analyzes the sector's response strategies. The study reveals a significant escalation in cyber threats, driven by the rapid digital transformation in banking

services and the increasing sophistication of cybercriminals. Key challenges include the digital literacy gap among customers and the evolving nature of cyber threats.

Babajide and Shoetan (2024) investigated cybersecurity challenges and strategies within the financial sectors of the United States of America (USA) and Nigeria, offering a comprehensive review and comparative analysis of these two nations. The study elucidates the complexities and variances in cybersecurity practices, focusing on how each country safeguards its financial data against increasing cyber threats. The review reveals that while the USA's financial sector benefits from advanced cybersecurity technologies and a robust regulatory framework, it still faces challenges related to sophisticated cyber-attacks and insider threat management. On the other hand, Nigeria's financial sector struggles with limited cybersecurity awareness, technological constraints, and evolving regulatory frameworks. Despite these differences, the study highlights that both countries share the critical need to enhance their cybersecurity posture to effectively address the evolving nature of cyber threats.

Iyoha et al. (2024) investigated the effect of security challenges on business operations and investment in Nigeria, focusing on various forms of insecurity, including Boko Haram, Fulani herdsmen, armed banditry, and kidnapping. These security issues have exacerbated fears among the populace, further compounded by hunger, unemployment, and inadequate infrastructure. The study adopts the frustration-aggression analysis and relies primarily on secondary data to explore the implications of these security problems on business activities in Nigeria. The researchers identify the root causes of insecurity that have hindered business operations and highlight the specific security challenges confronting the country. The study emphasizes that security challenges pose a significant threat to lives and properties, disrupt business activities, and discourage both local and foreign investment, ultimately hindering the socio-economic development of Nigeria.

Olaniyi et al. (2023) investigated the role of information governance (IG) in enhancing the robustness of the Nigerian banking industry, which is regulated by the Central Bank of Nigeria (CBN). The researchers employed a mixed-methods approach, using both qualitative and quantitative data, to explore the feasibility of implementing an Information Governance Framework (IGF) in the financial sector. Quantitative data from

the Nigerian Deposit Insurance Corporation (NDIC) revealed that effective IG programs are crucial for profitability in the banking industry. The study also included a case study of Capital One, demonstrating that appropriate governance policies could have either fully mitigated a cyber attack or significantly reduced its impact by minimizing the time hackers had unauthorized access. The results emphasize that effective IG relies on formalized structures, accountability, privacy, ethics, transparency, monitoring, compliance, and suitability. The study concludes with 95% confidence that while IG policies do not directly mitigate data breaches, they play a critical role in improving profitability by safeguarding assets, suggesting that financial institutions can leverage IG to protect against data breaches and enhance profitability.

Onunka et al. (2023) investigated the cybersecurity dynamics within the banking sectors of the United States (U.S.) and Nigeria, highlighting the profound significance of robust cybersecurity measures in safeguarding financial institutions amid the digital transformation of the global financial landscape. Having compared the U.S. and Nigerian banking systems, the research reveals distinct challenges and solutions faced by each country: while the U.S. contends with issues like money laundering and the need for increased competition, Nigeria's banking sector is shaped by factors such as the potential of Islamic banking and challenges related to financial inclusion. The study stresses the role of emerging technologies, especially artificial intelligence, in predicting, detecting, and responding to threats in real-time, though it cautions that these advancements also introduce new challenges as adversaries leverage them for more sophisticated attacks.

Opka et al. (2023) investigated the impact of Business Email Compromise (BEC) scams on economic sustainability within corporate organizations in Cross River State, Nigeria, a topic that has been relatively underexplored despite numerous studies on cybercrime. The study utilized a mixed-methods approach, collecting data through structured questionnaires and in-depth interviews with staff (n=1087). The data were analyzed using descriptive statistics, logistic regression, and content analysis. The findings revealed a significant increase in BEC victimization, which has adversely affected key corporate organizations, including banks, telecommunications firms, and manufacturing companies. The study also highlighted that the type of organization one

works for plays a crucial role in determining vulnerability to BEC scamming, suggesting that different sectors face varying levels of risk.

Akintoye et al. (2022) investigated the relationship between cybersecurity and financial innovation within Deposit Money Banks in Nigeria, focusing on the role of financial innovation in addressing the challenges posed by a growing population and reducing financial exclusion. The study underscores the importance of financial innovation but highlights that poor design, vulnerabilities, and inadequate adoption of new financial technologies have impeded progress. Using a survey research design, data were collected through structured questionnaires administered to senior staff members from 56 selected Deposit Money Banks. The findings revealed a significant and positive impact of cybersecurity measures, particularly in risk management and bank monitoring, on financial innovation in these banks. Based on these results, the study recommends the regular review and strengthening of risk management frameworks and enhanced monitoring of e-banking channels to bolster financial innovation and ensure transaction reliability.

Methodology

Research Design

The research design used for this study is the mixed-method research design, which combines both qualitative and quantitative approaches. This design is chosen to provide a comprehensive understanding of cyber risks and the emerging cyber insurance market in Nigeria. The qualitative component, involving in-depth interviews and case studies, allows for exploring the experiences and perspectives of key stakeholders, while the quantitative component, through structured surveys, enables the analysis of trends and correlations across a broader population. The mixed-methods approach ensures a holistic analysis, validating findings through multiple data sources and offering both depth and breadth to the study, making it well-suited.

Population of the Study

The population of this study comprises businesses operating in various sectors within Nigeria, including but not limited to finance, telecommunications, manufacturing, retail, and technology. Additionally, the study targets key stakeholders such as cybersecurity experts, insurance providers offering cyber insurance products, IT managers, and senior executives responsible

for risk management in these organizations. This diverse population is selected to capture a broad perspective on the impact of cyber risks, the level of awareness, and the adoption of cyber insurance across different industries, providing a comprehensive view of the emerging cyber insurance market in Nigeria.

Sampling Size and Sampling Techniques

A total of 250 respondents were used in this study, exceeding the minimum requirement of 124 as determined by the G*Power analysis to ensure adequate statistical power. The sampling techniques employed included stratified random sampling and purposive sampling. Stratified random sampling was used to ensure representation across different sectors, such as finance, telecommunications, and manufacturing, thereby capturing diverse perspectives on cyber risks and insurance. Within each stratum, respondents were randomly selected to maintain randomness and reduce bias. Additionally, purposive sampling was utilized to specifically target key stakeholders, such as cybersecurity experts and insurance providers, whose understandings are crucial for the study. This combination of sampling techniques ensures both breadth and depth in the data collected, enhancing the study's validity.

Research Instrument

The study makes use of a structured questionnaire and semi-structured interview guides as its research instruments. The structured questionnaire, featuring both closed and scaled questions, is employed to collect quantitative data on cyber risks, awareness, and the adoption of cyber insurance among various businesses in Nigeria. In addition, semi-structured interview guides are utilized to conduct in-depth interviews with key stakeholders, including cybersecurity experts, IT managers, and insurance providers, to gather qualitative insights into the practical challenges and perceptions related to cyber risks and insurance. This combination of instruments enables a thorough examination of both quantitative trends and qualitative details.

Method of Data Analysis

The study employs a method of data analysis that includes descriptive analysis, correlation, and multiple regression. Descriptive analysis is utilized to examine the demographic characteristics of the respondents, providing a clear overview of their background and profiles. Correlation analysis is then used to determine the relationships between key variables, such as

cyber risks and the adoption of cyber insurance. Additionally, multiple regression analysis is employed to assess the effect of these variables on the outcome measures, allowing for an evaluation of the strength and significance of their relationships and impacts. This approach ensures a comprehensive understanding of both the demographic context and the key factors influencing cyber insurance uptake.

Results

Demographic distribution of Respondents

Table 1 presents the demographic characteristics of the respondents, with detailed insights into their profiles. Among the 250 respondents, 64.4% were male, 33.2% were female, and 2.4% chose not to disclose their gender, ensuring a diverse representation. Age distribution showed 7.6% were under 25 years old, 30.4% were between 25 and 40 years old, 44.4% were between 41 and 54 years old, and 17.2% were 55 years and older, indicating a significant input from the 41-54 age group. Educational backgrounds varied, with 12.4% classified as "Others," 20.8% holding NCE/ND certificates, 29.6% with HND/BSc degrees, and 37.2% having postgraduate degrees, suggesting a well-informed respondent pool. Employment status revealed that 65.6% were full-time employees, 22.8% were part-time, and 11.6% were self-employed, reflecting diverse professional experiences. Work experience ranged from 11.2% with less than 5 years, 18.4% with 5-10 years, 43.6% with 11-15 years, to 26.8% with over 16 years, indicating a rich blend of insights from both seasoned and newer professionals.

Table 1: Demographic distribution of Respondents

	Frequency	Percentage
Gender of Respondent	161	64.4
Male		
Female	83	33.2
Prefer not to say	6	2.4
Total	**250**	**100**
Age of Respondent		
Less than 25 years	19	7.6
25-40 years	77	30.4
41 – 54 years	111	44.4

55 years and above	43	17.2
Total	**250**	**100**
Educational Level		
Others	31	12.4
NCE/ND Certificate	52	20.8
HND/BSc Certificate	74	29.6
Postgraduate	93	37.2
Total	**250**	**100**
Employment Status		
Full Time	164	65.6
Part Time	57	22.8
Self Employed	29	11.6
Total	**250**	**100**
Years of Work Experience		
Less than 5 years	28	11.2
5-10 Years	46	18.4
11 – 15 years	109	43.6
16years and above	67	26.8
Total	**250**	**100**

Source: Field survey, 2024

Test of Hypotheses

Hypothesis 1

$H0_1$: The level of cyber risk exposure experienced by Nigerian businesses does not significantly affect their financial security and operational continuity.

Table 2 displays the results of a linear regression analysis that explored the impact of cyber risk exposure on the financial security and operational continuity of businesses in Nigeria. The analysis shows a significant effect of cyber risk exposure, with results indicating ($F(1, 249) = 199.803$, $\rho < 0.05$, $R = 0.668$, $R^2 = 0.446$, and adjusted $R^2 = 0.444$. This suggests that approximately 45% of the variation in financial security and

operational continuity is explained by cyber risk exposure. The predictor's contribution is notably negative, with a coefficient (β = -0.706, $p < 0.001$), highlighting that increased exposure to cyber risks adversely affects financial security and operational continuity. The significant F-statistic confirms the overall model's validity, leading to the rejection of the null hypothesis that cyber risk exposure has no significant effect on these aspects of business. The finding is in line with Chidukwani, (2022) study on the Cyber Security of Small-to-Medium Businesses as well as Kumar and Mallipeddi, (2022) study that concluded that cyber risks reduces financial operation of small business.

Table 2: Effect of cyber risks exposure on financial security and operational continuity of business

	R	R-Squared	Adjusted R^2	F-value	Sig. of F	Decision
	.668	.446	.444	199.803	0.000	Sig.
	Coefficients	**Standard Error**	**t Stat**	**p-value**		
Constant	.526	.088	5.992	.000		
Cyber risks exposure	-.706	.050	-14.135	.000		

Source: Author's computation, 2024

Dependent variable: Financial security and operational continuity

Hypothesis 2

$H0_2$: There is no significant relationship between the size of a business and the demand for cyber insurance among Nigerian businesses.

Table 3 reports the results of a Pearson product-moment correlation analysis, aimed at investigating the relationship between business size and the demand for cyber insurance among Nigerian businesses. The analysis reveals a significant positive correlation ($R = 0.644^{**}$, $N = 250$, $p < 0.05$), suggesting that larger businesses are more likely to seek higher levels of cyber

insurance. This implies that as businesses grow in size, their demand for cyber insurance increases correspondingly. The correlation coefficient, which indicates a moderate effect size according to Cohen's guidelines (1988), underscores the strength of this relationship. Therefore, the findings lead to the rejection of the null hypothesis, which posited no significant relationship between business size and the demand for cyber insurance, affirming that a significant relationship does exist. The study support the outcomes by (Okpa, et al, 2022)

Table 3: relationship between business size and demand for cyber insurance

Items	Mean	Minimum	Maximum	N	R	ρ
Size of business	1.670	1.00	3.80	250	.644***	0.05
Demand for cyber insurance	1.615	1.00	3.40	250		

Source: Author's computation, 2024

Hypothesis 3

H_{03}**:** here is no significant difference in the effectiveness of Nigerian businesses that invest in cyber insurance compared to those that do not.

To address the objective of determining whether there is a significant difference in the effectiveness of performance between Nigerian businesses that invest in cyber insurance and those that do not, a paired sample t-test was conducted. The results, presented in Table 4, reveal a significant difference in performance effectiveness between the two groups (Crit–t = 2.306, Cal–t = -20.121, df = 1, $\rho < 0.05$). This finding indicates that businesses that invest in cyber insurance demonstrate significantly better performance compared to those that do not. As a result, the null hypothesis, which stated that there is no significant difference between businesses that invest in cyber insurance and those that do not, is rejected. The study concludes that cyber insurance investment positively impacts the effectiveness of business performance, highlighting the importance of such investments for Nigerian businesses. The study supported the outcome by Demirkan, et al (2020)

Table 4: Paired sample t-test result

Variable	N	Mean	Std	Crit-t	Cal-t	DF	ρ

business with cyber risks	250	1.978	0.476	2.306	-20.121	1, 249	0.00
business without cyber risks		2.329	0.587				

Source: Author, 2024

Hypothesis 4

$H0_4$: The level of cyber risk exposure does not have a significant impact on the profitability of Nigerian businesses.

Table 5 presents the results of a linear regression analysis assessing the impact of cyber risk exposure on the profitability of Nigerian businesses. The analysis indicates a significant effect of cyber risk exposure on profitability, with the model showing an F-statistic of $F(1, 249) = 179.482$, $\rho < 0.05$, $R = 0.648$, $R^2 = 0.420$, and adjusted $R^2 = 0.418$. The coefficient of determination R^2 suggests that approximately 42% of the variation in profitability among Nigerian businesses can be attributed to cyber risk exposure. The results further reveal that an increase in cyber risk exposure negatively affects profitability, with a unit increase in cyber risks reducing profitability by .693 as presented ($\beta = -0.693$, $p < 0.005$). The significant F-statistics value confirms that the regression model is robust, leading to the rejection of the null hypothesis that cyber risk exposure has no significant effect on the profitability of Nigerian businesses. The study supported the findings by Tam et al, (2021).

Table 5: Effect of cyber risks exposure on profitability

	R	**R-Squared**	**Adjusted R^2**	**F-value**	**Sig. of F**	**Decision**
	.648	.420	.418	179.482	0.000	Sig.
	Coefficients	**Standard Error**	**t Stat**	**p-value**		
Constant	.792	.091	8.716	.000		
Cyber risks exposure	-.693	.052	-13.397	.000		

Source: Author's computation, 2024

Dependent Variable: Profitability

Conclusion and Recommendations

This study investigated the impact of cyber risk exposure on the financial security, operational continuity, profitability, and demand for cyber insurance among Nigerian businesses, utilizing a sample of 250 respondents. The primary objectives were to examine the effect of cyber risk exposure on financial stability and operational effectiveness, analyze the relationship between business size and cyber insurance demand, assess the differences in performance between businesses investing in cyber insurance and those not investing, and evaluate how cyber risk exposure affects profitability. The study employed mixed-methods research design, including descriptive analysis, correlation, and regression techniques to analyze the data.

The findings concluded that cyber risk exposure significantly impacts the financial security and operational continuity of Nigerian businesses, with a notable negative effect on profitability. A significant positive relationship was identified between business size and the demand for cyber insurance, indicating that larger businesses are more likely to invest in such insurance. Moreover, there was a significant difference in effectiveness between businesses that invested in cyber insurance and those that did not, highlighting the benefits of insurance in enhancing business performance. Based on these outcomes, it is recommended that Nigerian businesses invest in robust cyber insurance policies to mitigate risks and safeguard profitability. Additionally, businesses should strengthen their cybersecurity measures and regularly review risk management frameworks to enhance resilience against cyber threats. Policymakers and regulatory bodies are encouraged to develop and implement comprehensive guidelines to support businesses in managing cyber risks effectively

References

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.

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.

Alabi, A., Bamidele, A. H., & Oladimeji, A. B. (2023). Cybercrime in Nigeria: Social Influence Affecting the Prevention and Control. *LAFIA JOURNAL OF ECONOMICS AND MANAGEMENT SCIENCES*, *8*, 227-241.

Albustanji, H. (2024). COVID-19 Pandemic Impact on Cyber Threats. *Faculty of Organisation Studies in Novo mesto, Slovenia*, 48.

AL-Hawamleh, A. (2024). Cyber resilience framework: Strengthening defenses and enhancing continuity in business security. *International Journal of Computing and Digital Systems*, *15*(1), 1315-1331.

Arenas, Á., Ray, G., Hidalgo, A., & Urueña, A. (2024). How to keep your information secure? Toward a better understanding of users security behavior. *Technological Forecasting and Social Change*, *198*, 123028.

Arenas, Á., Ray, G., Hidalgo, A., & Urueña, A. (2024). How to keep your information secure? Toward a better understanding of users security behavior. *Technological Forecasting and Social Change*, *198*, 123028.

Bekkers, L., van't Hoff-De Goede, S., Misana-ter Huurne, E., van Houten, Y., Spithoven, R., & Leukfeldt, E. R. (2023). Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model. *Computers & Security*, *127*, 103099.

Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: challenges, research focus and recommendations. *IEEE Access*, *10*, 85701-85719.

Choudhary, A., Choudhary, G., Pareek, K., Kunndra, C., Luthra, J., & Dragoni, N. (2022). Emerging cyber security challenges after COVID pandemic: a survey. *Journal of Internet Services and Information Security*, *12*(2), 21-50.

Cortez, E. K., & Dekker, M. (2022). A corporate governance approach to cybersecurity risk disclosure.

European Journal of Risk Regulation, *13*(3), 443-463.

Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. *Journal of Management Analytics*, *7*(2), 189-208.

Ebekozien, A., Aigbavboa, C., & Samsurijan, M. S. (2023). An appraisal of blockchain technology relevance in the 21st century Nigerian construction industry: perspective from the built environment professionals. *Journal of Global Operations and Strategic Sourcing*, *16*(1), 142-160.

Ezati Rad, R., Mohseni, S., Kamalzadeh Takhti, H., Hassani Azad, M., Shahabi, N., Aghamolaei, T., & Norozian, F. (2021). Application of the protection motivation theory for predicting COVID-19 preventive behaviors in Hormozgan, Iran: a cross-sectional study. *BMC Public Health*, *21*, 1-11.

Familoni, B. T., & Shoetan, P. O. (2024). Cybersecurity in the financial sector: a comparative analysis of the USA and Nigeria. *Computer Science & IT Research Journal*, *5*(4), 850-877.

George, A. S., Baskar, T., & Srikaanth, P. B. (2024). Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors. *Partners Universal International Innovation Journal*, *2*(1), 51-75.

Hassan, A. O., Ewuga, S. K., Abdul, A. A., Abrahams, T. O., Oladeinde, M., & Dawodu, S. O. (2024). Cybersecurity in banking: a global perspective with a focus on Nigerian practices. *Computer Science & IT Research Journal*, *5*(1), 41-59.

Hassan, A. O., Ewuga, S. K., Abdul, A. A., Abrahams, T. O., Oladeinde, M., & Dawodu, S. O. (2024). Cybersecurity in banking: a global perspective with a focus on Nigerian practices. *Computer Science & IT Research Journal*, *5*(1), 41-59.

Ibiyemi, M. O., & Olutimehin, D. O. (2024). Cybersecurity in supply chains: Addressing emerging threats with strategic measures. *International Journal of Management & Entrepreneurship Research*, *6*(6).

Kala, E. M. (2023). The impact of cyber security on business: how to protect your business. *Open Journal of Safety*

Science and Technology, *13*(2), 51-65.

Kanu, I. A., Adidi, D. T., & Kanu, C. C. (2024). Artificial intelligence and cybercrime in Nigeria: Towards an Ethical framework. *Dialogue and Universalism*, *34*(1), 207-221.

Kayode-Ajala, O. (2023). Applications of Cyber Threat Intelligence (CTI) in financial institutions and challenges in its adoption. *Applied Research in Artificial Intelligence and Cloud Computing*, *6*(8), 1-21.

Khan, N. F., Ikram, N., Murtaza, H., & Javed, M. (2023). Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's Model. *Computers & Security*, *125*, 103049.

Kineber, A. F., Oke, A., Aliu, J., Hamed, M. M., & Oputu, E. (2023). Exploring the adoption of cyber (digital) technology for sustainable construction: a structural equation modeling of critical success factors. *Sustainability*, *15*(6), 5043

Kumar, S., & Mallipeddi, R. R. (2022). Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions. *Production and Operations Management*, *31*(12), 4488-4500.

Meshram, B. B., & Singh, M. K. (2024). Cyberguard: Cybercrime Risk Management And Insurance, Compensation, Punishment Model In The Digital Realm. *Educational Administration: Theory and Practice*, *30*(6), 4294-4322.

Okoru, A. O., & Oluku, O. (2024). Cybercrime, Crime Security and National Development in Nigeria. *FUOYE JOURNAL OF CRIMINOLOGY AND SECURITY STUDIES*, *3*(2).

Okpa, J. T., Ajah, B. O., Nzeakor, O. F., Eshiotse, E., & Abang, T. A. (2023). Business e-mail compromise scam, cyber victimization, and economic sustainability of corporate organizations in Nigeria. *Security Journal*, *36*(2), 350-372

Okpa, J. T., Ajah, B. O., Nzeakor, O. F., Eshiotse, E., & Abang, T. A. (2022). Business e-mail compromise scam, cyber victimization, and economic sustainability of corporate organizations in Nigeria. *Security Journal*, 1-23

Olaiya, O. P., Adesoga, T. O., Ojo, A., Olagunju, O. D., Ajayi, O. O., & Adebayo, Y. O. (2024). Cybersecurity strategies in fintech: safeguarding financial data and assets. *GSC Advanced Research and Reviews*, *20*(1), 050-056.

Olaniyi, O. O., Olaoye, O. O., & Okunleye, O. J. (2023). Effects of Information Governance (IG) on profitability in the Nigerian banking sector. *Asian Journal of Economics, Business and Accounting*, *23*(18), 22-35.

Onunka, O., Alabi, A. M., Okafor, C. M., Obiki-Osafiele, A. N., Onunka, T., & Daraojimba, C. (2023). Cybersecurity in US and Nigeria banking and financial institutions: review and assessing risks and economic impacts. *Advances in Management*, *1*.

Pugnetti, C., Björck, A., Schönauer, R., & Casián, C. (2024). Towards Diagnosing and Mitigating Behavioral Cyber Risks. *Risks*, *12*(7), 116.

Reis, O., Oliha, J. S., Osasona, F., & Obi, O. C. (2024). Cybersecurity dynamics in Nigerian banking: trends and strategies review. *Computer Science & IT Research Journal*, *5*(2), 336-364.

Schwieger, D., & Ladwig, C. (2022). Cyber Insurance Concepts for the MIS and Business Curriculum. *Information Systems Education Journal*, *20*(5), 54-66.

Strupczewski, G. (2021). Defining cyber risk. *Safety science, 135*, 105143.

Tam, T., Rao, A., & Hall, J. (2021). The good, the bad and the missing: A Narrative review of cyber-security implications for Australian small businesses. *Computers & Security*, *109*, 102385.

Temara, S. (2024). The Ransomware Epidemic: Recent Cybersecurity Incidents Demystified. *Asian Journal of Advanced Research and Reports*, *18*(3), 1-16.

Thakur, M. (2024). Cyber security threats and countermeasures in digital age. *Journal of Applied Science and Education (JASE)*, *4*(1), 1-20.

Udo, W. S., Ochuba, N. A., Akinrinola, O., & Ololade, Y. J. (2024). Conceptualizing emerging technologies and ICT adoption: Trends and challenges in Africa-US contexts. *World Journal of Advanced*

Research and Reviews, *21*(3), 1676-1683.

Wang, V., Nnaji, H., & Jung, J. (2020). Internet banking in Nigeria: Cyber security breaches, practices and capability. *International Journal of Law, Crime and Justice*, *62*, 100415.