Global Research Journal of Management and Social Sciences (GRJMSS)
Volume.16, Number 6; June-2025;
ISSN: 2836-9181| Impact Factor: 9.65
https://zapjournals.com/Journals/index.php/grjmss
Published By: Zendo Academic Publishing

EFFECT OF CYBER SECURITY ON GROWTH OF INSURANCE INDUSTRY IN NIGERIA, 2009-2024

[1]Okparaka, Vincent Chukwuka (Ph.D.), [2]Udeji, Banabas Uchenna and [3]Sir Henry Ofordile (Ph.D. Fcna, Acit, Ficpan, Frcn, Trcn)

Article Info
Keywords: Cyber, Growth, Industry, Insurance, Security

DOI
10.5281/zenodo.15585889

Abstract
The aim of study was to examine the effect of cyber security on growth of insurance industry in Nigeria. Specific objectives were to: examine the effect of web-pay-code programs on gross premium income of insurance industry in Nigeria and investigate the effect of mobile pay code on gross premium of insurance industry in Nigeria. Ex post facto research design was adopted. Study used time series data (2009-2024) within the periods under review, which was obtained from Central Bank of Nigeria (CBN) statistical bulletin. Ordinary least square (OLS) regression model was used to test formulated hypotheses. The findings revealed web-pay code had a positive and significant effect on growth of insurance industry proxied by gross premium income in Nigeria (coff =0.088429, pv<0.05) and mobile pay code had a positive and significant effect on the growth of insurance business proxied by gross premium income in Nigeria (coff=0.112788, pv<0.05). In light of the findings, the study concluded that cyber security had positive and significant effect on growth of insurance industry in Nigeria. Based on the findings, the following recommendations were made, Nigerian businesses invest in robust cyber insurance policies to mitigate risks and safeguard profitability through introduction of web-pay code programs. Additionally, businesses should strengthen their cyber security measures and regularly review risk management on mobile pay code frameworks to enhance resilience against cyber threats.

1.1 Introduction

Technology-based solutions are being adopted by organizations around the world, making the world a digital place. Because of this, the risk of cybercrime has increased, and this is especially true if the controls that are in

[12]Department of Insurance and Risk Management, Enugu State University of Science and Technology, ESUT
[3]Coal City University Enugu State, Nigeria.

place are insufficient or nonexistent. Incidents involving cyber risk can have a diverse range of effects on the businesses that are impacted by them. According to the Allianz Risk Barometer for 2019 and 2020, cyber risk, in conjunction with business interruption that is primarily caused by cyber risk occurrences, has been identified as the most critical risk facing businesses around the world.

The practices of cyber security risk management help the insurance industry perform better by increasing client trust and strengthening data security and privacy, which ultimately leads to more potential for revenue, (Gatzert & Schubert, 2022). Cyber security refers to a series of practices and activities fashioned out with a view to ensuring the protection of personal and organizational data, information and networks from all possible threats whether internally or externally induced (Beck, Chen, Lin, & Song, 2014; Li & Liu 2021).

Cyber risk is the potential for loss or harm as a result of compromising an organization's technological infrastructure. Cyber risk is associated with online activity, electronic commerce, information systems, networks, and data storage, and it refers to the potential for these things to be compromised (RSA, 2016). Threats and incidents related to cyber security are seen as having a greater potential for harm by larger companies, and as a result, adequate investments are made in the growth of counter measures.

During the course of the last decade, cyber-attacks on insurance companies have undergone a dramatic transformation as a result of the rise in their level of technical sophistication, frequency, and severity. Even though the majority of insurance companies have put in place a high level of cyber security precautions, the number of cyber-attacks continues to rise. This not only demonstrates the inevitability of cyber-attacks, but also the difficulty of completely guaranteeing the integrity of financial systems in insurance companies. More than half of the world's commercial banks have been the target of at least one type of cyber-attack, as stated by Security Intelligence Solutions (2020).

The primary objective of cybercrime is to cause disruption to normal business operations as well as essential infrastructure. Data that has been illegally obtained is frequently utilized by cyber criminals for the purposes of financial gain, the infliction of financial loss, the damage of a person's reputation, the accomplishment of military objectives, or the dissemination of religious or political ideologies. Some hackers don't require a justification to hack; rather, they do it solely for the purpose of demonstrating their expertise (Tariq, 2018).

As a result of the rapid pace at which businesses are implementing digital transformations with the help of mobile devices, cloud services, social media, and Internet of Things services, enterprise risk management has shifted its primary emphasis to cyber security. Better cyber security leads to increased consumer trust and income potential, but requirements for data protection and privacy are continually growing, making it more difficult to manage cyber security (Lee, 2021).

One of the strategies for managing the risks associated with cyber security is limiting data access. This is done to avoid putting sensitive information at risk. Cyber security refers to a collection of technologies, processes, practices, and response and mitigation measures that are designed to protect networks, computers, programs, and data from being compromised, damaged, or inappropriately accessed. It also aims to maintain the confidentiality, integrity, and availability of this information (Panda & Bower, 2020).

In today's increasingly digital world, the importance of maintaining strong cyber security can be attributed to a number of factors, including the following: Cyber-attacks can be extremely expensive for businesses; in addition to monetary losses, a data breach can result in irreparable damage to a company's reputation. In addition, cyber-attacks are becoming increasingly damaging as time goes on. The methods that cybercriminals use to launch cyber-attacks are becoming increasingly sophisticated as time goes on. As a result of regulations such as GDPR, companies are being put under increased pressure to improve the security of the personally identifiable information that they store. Because of the factors mentioned above, cyber security has emerged as an essential

component of the company, and the primary focus now is on developing appropriate response plans that lessen the negative effects of cyber-attacks, (Tariq, 2018).

Insurance as a financial intermediary plays a significant role in economic growth of any country (Srijana & Fatta, 2017). The history of insurance dates back to the ancient era of civilization, well before the current economic and monetary system. Insurance existed in a multitude of forms, with the earliest dating back to the 2nd and 3r dmillennia BC. Babylonian, Chinese, and Indian traders would redistribute their goods among many different ships used to transport goods across the ocean. This practice was driven by the uncertainty of traversing treacherous waters, ensuring that if one ship overturned, all the goods would not be lost. Insurance stimulates business activities to operate cost-effectively (Ibegbulem, 2021; Agbamuche, 2012). Ubom (2012), the primary aim of insurance is to provide customers with safeguards against risks that may result in significant losses, such as job or income loss, inability to maintain social amenities and a decline in purchasing power.

It is critical to implement the risk management practices for cyber security. On the other hand, there are circumstances in which they are not sufficient. Threats to a company's cyber security do exist, and businesses can and do fall prey to them. It's common for incident response plans to consist of nothing more than a contact person, which is inefficient. Techniques for the management of cyber security risks need to be consistently implemented in order for them to be effective. Based on this, the study seeks to examine the effect of cyber security on growth of insurance industry in Nigeria from 2009 to 2024

Statement of the Problem

The safeguard of system and internet-connected systems, such as software, hardware and data, from cyber-attacks, is referred to as cyber security. Individuals and businesses employ the technique to guard against illegal access to data centers and other digital systems. The internet has made the world smaller in many ways but has equally opened up the business world to influences that have never before been so varied and so challenging. As fast as the business can grow through the help of information communication technology, internet security challenges are unavoidable as data hackers grow even faster (Seemma, Nandhini & Sowmiya, 2018).

In emerging economies such as Nigeria, risk management has relied primarily on a reactive approach to risk financing for years, which has grown more unsustainable due to a variety of factors. The recent economic meltdown orchestrated by Covid-19 and the constant attack on insurance facilities by cybercrime syndicates has raised serious questions about the growth of financial service industries like insurance in Nigeria. Anoke, Nzewi, Agagbo, and Onu (2021) noted that the vulnerability of insurance firms in Nigeria is increasing as emerging economies grow and accumulate more assets as well as the increase in the exposure to the internet which points to a continuing trend of increasing losses due to cybercrime and cyber-related issues.

The growing threat of cyber-attacks has placed the insurance industry at a critical crossroads. Insurance companies handle vast amounts of sensitive customer data ranging from financial details to medical records making them prime targets for cybercriminals. With breaches becoming more sophisticated and costly, the risks are no longer just financial. A single attack can cripple operations, damage reputations, and trigger regulatory penalties. Cyberspace is a difficult environment that is always changing and evolving. As a result, personnel in charge of security in diverse sectors face problems in keeping up with advances in the cyber realm. A stable, safe, and strong cyberspace is critical for economic growth and sustainability, especially in the insurance sector. As a result, insurance companies in Nigeria have continuously invested in cyber security to protect their database, prevent monetary losses, maintain company image and remain afloat in a competitive business environment. However, despite this huge investment made by Nigerian insurance firms, cyber criminals still attack, penetrate and have undue access to their cyber-space causing damages to both the institution and customers of the insurance industry.

However, this work therefore seeks to fill this gap by examining cyber security (web-pay code and mobile pay code) and growth of insurance industry in Nigeria from 2009 to 2024. Based on the above, the study examines cyber security (web-pay code and mobile pay code) on growth of insurance industry in Nigeria from 2009 to 2024.

Objectives of the Study

The main objective of the study was to examine the effect of cyber security on growth of insurance industry in Nigeria. Specific objectives were to:

i. Examine the effect of web-pay-code programs on gross premium income of insurance industry in Nigeria.
ii. Investigate the effect of mobile pay code on gross premium of insurance industry in Nigeria.

REVIEW OF RELATED LITERATURE

Cyber Security

Cyber security refers to a series of practices and activities fashioned out with a view to ensuring the protection of personal and organizational data, information and networks from all possible threats whether internally or externally induced (Beck, Chen, Lin, & Song, 2014; Li & Liu 2021; Umar, 2019; Morgan, 2020). Bob- Alli (2010) opined that individuals, businesses, and the government all suffer as a result of these losses, which include welfare losses, business interruption, profit reduction/increased operational costs, and revenue losses, among other things.

Web-Pay-Code Programs

Web-pay code provides instructions and information on using the Interswitch WebPAY platform for online payments. It typically covers aspects like setting up a WebPay account, making payments, and managing payment history. These guides are usually designed to help users navigate the payment process effectively and securely in order to keep security of transaction in insurance businesses (Gardner & Thomas, 2014).

Mobile Pay Code

A Mobile Pay Code, also known as a unique transaction reference, is a code generated by the mobile payment system to identify and track specific transactions security. This code ensures the integrity and security of each payment made through a mobile payment system under the insurance businesses are well secured (Cengage, 2019; ManageEngine, 2019; Rouse, 2017).

Insurance

Insurance is a means of protection from financial loss. It is a form of risk management, primarily used to hedge against the risk of a contingent or uncertain loss. An entity which provides insurance is known as an insurer, insurance company, insurance carrier or underwriter (John, et al, 2022).

Growth of Insurance Industry

The insurance industry in Nigeria has shown positive growth, particularly in premium generation and asset expansion, but still faces challenges in penetration. The industry has experienced significant increases in gross premium written and total assets, but its penetration rate remains below one percent compared to other African countries (John, et al, 2022).

Theoretical Framework

This study was anchored significantly on Protection Motivation and Growth theory of Insurance in Nigeria.

Protection Motivation Theory

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, cyber security, 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). 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.

Empirical Review

The relationship between cyber security and growth of insurance industry in the world especially in Nigeria has been widely studied in the past few years. This is because the negative impact of cyber-crime and internet fraud stars is causing untold hardship not only to the insurance sector but to the financial institutions the world over. Some of the findings of the empirical studies are reviewed in this section.

In a similar study, Abdulrahim, (2019) determined the key cyber security risks being faced by Kenyan SMEs and to develop an implementation strategy which will provide a roadmap for managing cyber risk as a business risk. The research findings revealed that cyber security investment, web-pay code, training and awareness, cyber security policy programs, cyber security vulnerability management programs, real time network monitoring and incident management play a big role in the management of Cyber -risk within SMEs.

In the same vein, Ogene (2024) addresses Nigeria's critical cyber security challenges and the urgent need for strategic investment to safeguard its digital economy. This study employed a mixed-methods approach, analyzing academic literature, case studies, and reports on Nigeria's cyber security landscape. The findings indicate that investment in governance, skilled personnel, and emerging technologies is crucial for mitigating these risks.

Following the view of Okolo, Arume and Adedayo, (2024) investigated this relationship within Nigeria's Deposit Money Banks, employing a comprehensive analysis of key variables such as compliance adherence, web-pay code, training completion rate, risk awareness and management, behavioral analytics, employee feedback and engagement, and incident response time. The study revealed that compliance adherence, training completion rate, and risk awareness and management significantly influenced employee feedback and engagement.

According to Ajufo and Qutieshat (2023) shed light on the human factors influencing cyber security in Nigerian banks. They identify social engineering, poor information security culture, risky password practices, stress, web-pay code, burnout, and security fatigue as critical factors contributing to successful cyber-attacks. The study emphasizes the importance of cyber security awareness and training in mitigating these human-related vulnerabilities, providing practical recommendations for Nigerian banks to enhance their cyber security posture.

Aforementioned opinion by Abduel, (2024) assessed users' awareness of cyber security practices for preventing data attacks. The study employed a descriptive research design and quantitative research approach. Findings revealed that the user's awareness of cyber security practices on prevention of data attacks was high in the selected case for study, which remains anonymous.

Following previous study by Srinivas, Das, and Kumar (2019) examined government regulations in cyber security, highlighting the complexity of new technologies and the uncertainty in their adoption. Their study suggested that cyber security awareness plays a crucial role in shaping attitudes and intentions toward learning and using the latest technologies.

Emem and Ubong, (2022) examined the effect of insurance mobile pay on deepening insurance services in Nigeria. The researcher employed the use of survey research design in which primary data was obtained through questionnaire administration. The finding was that there is a significant effect of the application of transaction

processing system on deepening of insurance services in Nigeria. There is a significant influence of the use of decision support system on deepening of insurance services in Nigeria. There is a significant influence of the adoption of office automation system on deepening of insurance services in Nigeria.

John, et al (2024) studied the role of insurance industry on economic growth in Nigeria. Ex-post facto research design was applied. The data were analyzed using the Ordinary Least Square (OLS) method. From the analysis, it was revealed that there was a significant relationship between insurance income and gross domestic product in Nigeria. It was further discovered that there was a significant relationship between insurance premium and gross domestic product in Nigeria. Total insurance investment was also found to have a significant effect on gross domestic product in Nigeria.

Gaps in Empirical Review

Additionally, an empirical review was carried out where past and present studies both global and local were reviewed. In addition to the above, quite a number of gaps were identified easily from the previous studies reviewed such as; geography or area of the study is different from other studies, organizations used for the study may be different from other studies, and the variables studies may be different from other empirical examinations. Despite the numerous studies on cyber security, there is a dearth of studies that cover the two variables (Web-Pay Code and Mobile-Pay Code Programs) that were examined in this study. The study assessed the various variables so as to get a glimpse of the influence of cyber security on development of insurance industry. This aided in getting results and as a result closing the gap. In addition, the gap in empirical review is even more significant as more studies were centered in the Western developed countries, Few studies have been conducted on cyber security and development of insurance industry in Nigeria examples; cyber security and business sustainability of quoted insurance firms in Nigeria.

In addition, most studies have used survey research design, which limits the understanding of the complex relationship between variables. Secondly, none of the studies have measured the relationship between the independent and dependent variables beyond the sample period or provided insights into the relative importance of each variable in the model. Lastly, there are conflicting results from previous studies. This study aims to address these gaps by complementing previous research, exploring the dynamic relationship between cyber security and development of insurance industry in Nigeria using secondary data that includes two inputs: web-pay and mobile pay code. The study also estimate the magnitude of the relationship between these variables. It is therefore important that cyber security practices (Web-Pay Code and Mobile-Pay Code Programs) be examined to bring to light such interplay in this sector. These are the gaps that this present study seeks to fill.

METHODOLOGY

Research Design

The study used ex-post facto research design because it was suitable for the assessment of data before and after this study. The choice of design was based on the fact that it does not provide the study an opportunity to control the variables; mainly they have already occurred and cannot be manipulated.

Nature and Sources of Data

The study used time series data (2009-2024) within the periods under review. The study was longitudinal and data for this analysis are mostly from secondary sources. This was evidently true as data were obtained from the Central Bank of Nigeria (CBN) Statistical Bulletin from 2009 to 2024.

Model Specification

The study used a simple model relating all the variables under investigation. In order to investigate the relationship between cyber security and growth of insurance industry in Nigeria, Ordinary least square (OLS) regression model was used to test the effect of cyber security (independent variables) on growth of insurance industry in Nigerian

(dependent variable). A OLS model was used in line with model of John, et al (2022). John, et al (2022) model was adopted and re-specified/modified to capture the objectives of this present study. John, et al (2022) model was specified as follow:

GDP= f(NIC, PLI, NLP, TII,INF, u)…….. (1)

The functional relation of the model was given as:

GDP= β +β1NIC+ β2PLI + β3 NLP + β4TII + β5INF + u

Where; GDP= gross domestic product at market price

NIC= number of insurance companies in Nigeria

PLI= premium of life insurance companies

NLP= premium of non-life insurance companies

TII= total insurance investment

INF=inflation rate

In order to achieve the objective of this study, the models below were re-specified in line with the above model of Oke (2012). Thus, the general model for the study was stated as follow:

The functional relation of the model was given as:

$GPI = \beta_0 + \beta_1 WPC + \beta_2 MPI + \mu_i$ ---------- (ii)

Where:

GPI= Gross Premium Income.

WPC= Web-Pay Code Programs

MPC = Mobile Pay Code

$\beta_0$and β_2 =Parameters

μ – Error term

Method of Data Analysis

Data for the study was subjected to pretest before the main regression test was carried out to guard against getting spurious and misleading results, and ensure that the outcome of this study can be used for meaningful prediction. Such diagnostic test to be carried out include: Unit root test, correlation test, normality test, trend analysis and descriptive tests. Stationarity test was done using the Augmented Dickey-Fuller. Ordinary least square (OLS) regression model was used for data analysis if the variables are stationary at the same level. However, Hypotheses was tested at 5% level of significance and 95% confidence level. The decision rule shall be: Accept the null hypothesis if p-value of (t-statistic) is greater than (0.05) level of significance, otherwise accept the alternate hypothesis.

DATA PRESENTATION AND ANALYSES

Descriptive Statistics

Table 1 Descriptive Statistics

	LOGGPI	LOGMPC	LOGWPC
Mean	12.74810	6.284386	6.896107
Median	12.69500	6.360666	4.885525
Maximum	13.35572	12.30047	13.90821
Minimum	12.10038	0.239017	3.220874
Std. Dev.	0.423183	3.428470	4.035045
Skewness	-0.009893	-0.004192	0.916943
Kurtosis	1.742315	2.283015	2.049068

Jarque-Bera	0.988852	0.299914	2.667129
Probability	0.609921	0.860745	0.263536
Observations	15	15	15

Source: Extracted from E-View 10 Package

The descriptive statistics for the variables in Table 4.2.1 highlight key measures. The mean values indicate average figures, with Gross Premium Income (GPI) at 12.74810 ₦ billion, Web-Pay Code (WPC) at 6.896107 ₦ billion, Mobile Pay Code (INSFA) at 6.284386 ₦ billion. Therefore, Gross Premium Income was the highest mean average value among other related variables under the study.

Table 2 Correction Analysis

Correlation			
t-Statistic			
Probability	LOGGPI	LOGMPC	LOGWPC
LOGMPC	0.959467	1.000000	
	11.79356	-----	
	0.0000	-----	
LOGWPC	0.813253	0.836781	1.000000
	4.841285	5.294052	-----
	0.0004	0.0002	-----

Source: Extracted from E-View 10 Package

From the result, all the series share bivariate positive and significant correlation one with another and others share negative and non significant correlation with another. This is evidenced by the fact that their respective correlation coefficients are positive or negative and the probability values of the associated t-statistics respectively significant and non significant by all being less than 0.05 while same are high than 0.05.

Table 3 Test of Unit Root

Variables	**ADF**	**Cv @ 5%**	**Pv**	**Inference**
LGPI	**-1.23`**	**-3.11**	**>0.6305**	**Levels**
LWPC	**-4.10**	**-3.11**	**<0.00921**	**Difference**
LMPC	**-2.31**	**-3.87**	**>0.3972**	**Difference**

Source: Extracted from E-view 10.0

The Unit root test results show that the variables are integrated of different orders which justified introduction of Ordinary least square (OLS) regression model. LGPI was ordered at levels while LWPC and LMPC are ordered at difference.

Test of Hypotheses

Test of Hypothesis One

The hypotheses for this study shall be presented in their null and alternate forms.

H_{01}: Web-pay-code programs does not significantly affect gross premium income of insurance industry in Nigeria.

Dependent Variable: LOGGPI
Method: Least Squares
Date: 04/28/25 Time: 16:07
Sample: 2009 2023
Included observations: 15

Table 4: ARDL Result

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	12.13828	0.123885	97.98029	0.0000
LOGWPC	0.088429	0.015639	5.654477	0.0001
R-squared	0.710938	Mean dependent var		12.74810
Adjusted R-squared	0.688703	S.D. dependent var		0.423183
S.E. of regression	0.236111	Akaike info criterion		0.074534
Sum squared resid	0.724727	Schwarz criterion		0.168940
Log likelihood	1.440998	Hannan-Quinn criter.		0.073528
F-statistic	31.97311	Durbin-Watson stat		1.912194
Prob(F-statistic)	0.000079			

Source: Researcher's extract from E Views 10.0

From the OLS result shown above, WEB-PAY and gross premium income with an associated probability value of 0.0000. The result further revealed that 1 percent decrease in gross premium income will lead to about 12 percent increase in WEB-PAY. The R-square value of 71% shows that the independent variables jointly explain about 71% of the total variations in gross premium income while the remaining unexplained 1% might be attributable to other relevant variables not included in the model. The Durbin- Watson statistic value of 1.9 indicates that there was no autocorrelation problem in the model. The bases here was that coefficient showed positive sign while pv was less than 0.5% level of significant. Overall regression result indicates that F-sta = 31.97311 and pv = 0.00000 still showing significant nature of the result. **Decision Rule:** departing by the decision criteria to accept H_0 if the sign of the coefficient was positive. The study rejected H_0 and concluded that web-pay code had a positive and significant effect on growth of insurance industry proxied by gross premium income in Nigeria.

Test of Hypothesis Two

H_{02}: Mobile pay code does not significantly affect gross premium income of insurance industry in Nigeria.

Dependent Variable: LOGGPI
Method: Least Squares
Date: 04/28/25 Time: 16:08
Sample (adjusted): 2009 2022
Included observations: 14 after adjustments

Table 5: ARDL Result

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	11.99590	0.067900	176.6701	0.0000
LOGMPC	0.112788	0.009564	11.79356	0.0000
R-squared	0.920576	Mean dependent var		12.70470
Adjusted R-squared	0.913958	S.D. dependent var		0.403027

S.E. of regression	0.118220	Akaike info criterion	-1.300977
Sum squared resid	0.167711	Schwarz criterion	-1.209683
Log likelihood	11.10684	Hannan-Quinn criter.	-1.309428
F-statistic	139.0882	Durbin-Watson stat	1.301105
Prob(F-statistic)	0.000000		

Source: Researcher's extract from E Views 10.0

From the OLS regression result shown above, mobile pay code and gross premium income with an associated probability value of 0.0000. The result further revealed that 1 percent increase in gross premium income will lead to about 11 percent increase in MOBILE PAY CODE. The R-square value of 92% shows that the independent variables jointly explain about 92% of the total variations in gross premium income while the remaining unexplained 8% might be attributable to other relevant variables not included in the model. The Durbin- Watson statistic value of 1.30 indicates that there was no autocorrelation problem in the model. The bases here was that coefficient showed positive sign while pv was less than 0.5% level of significant. Overall regression result indicates that F-sta = 139.0882 and pv = 0.00000 still showing significant nature of the result. **Decision Rule:** departing by the decision criteria to accept H_0 if the sign of the coefficient was positive. The study rejected H_0 and concluded that mobile pay code had a positive and significant effect on the growth of insurance business proxied by gross premium income in Nigeria.

Discussion of Findings

Hypothesis One: Departing by the decision criteria to accept H_0 if the sign of the coefficient was positive. The study rejected H_0 and concluded that web-pay code had a positive and significant effect on growth of insurance industry proxied by gross premium income in Nigeria. This was in agreement with the study by a similar study, Abdulrahim, (2019) determined the key cyber security risks being faced by Kenyan SMEs and to develop an implementation strategy which will provide a roadmap for managing cyber risk as a business risk. The research findings revealed that cyber security investment, web-pay code, training and awareness, cyber security policy programs, cyber security vulnerability management programs, real time network monitoring and incident management play a big role in the management of Cyber -risk within SMEs.

Hypothesis Two: Departing by the decision criteria to accept H_0 if the sign of the coefficient was positive. The study rejected H_0 and concluded that mobile pay code had a positive and significant effect on the growth of insurance business proxied by gross premium income in Nigeria. This was in line with study by Emem and Ubong, (2022) examined the effect of insurance mobile pay on deepening insurance services in Nigeria. The researcher employed the used of survey research design in which primary data was obtained through questionnaire administration. The finding was that there was a significant effect of the application of transaction processing system on deepening of insurance services in Nigeria. There was a significant influence of the use of decision support system on deepening of insurance services in Nigeria. There was a significant influence of the adoption of office automation system on deepening of insurance services in Nigeria.

Summary of Findings

i. That web-pay code had a positive and significant effect on growth of insurance industry proxied by gross premium income in Nigeria (coff =0.088429, pv<0.05).

ii. That mobile pay code had a positive and significant effect on the growth of insurance business proxied by gross premium income in Nigeria (coff=0.112788, pv<0.05).

Conclusion

The study thus concludes that cyber security had positive and significant effect on growth of insurance industry in Nigeria. It was also concluded that web-pay code had a positive and significant effect on growth of insurance industry proxied by gross premium income in Nigeria and mobile pay code had a positive and significant effect on the growth of insurance business proxied by gross premium income in Nigeria.

Recommendations

Based on these outcomes, it was recommended that Nigerian businesses invest in robust cyber insurance policies to mitigate risks and safeguard profitability through introduction of web-pay code programs. Additionally, businesses should strengthen their cyber security measures and regularly review risk management on mobile pay code frameworks to enhance resilience against cyber threats.

Contribution to Knowledge

The study contributed to the existing literature on cyber security and growth of insurance industry and has also bridged the gap which existed between developed countries and developing countries with particular reference to Nigeria. Equally, the study made significant contributions to knowledge by providing a model in figure 5.1 below which shows the common link between cyber security and growth of insurance industry. The model was constructed based on researcher's findings from the study.

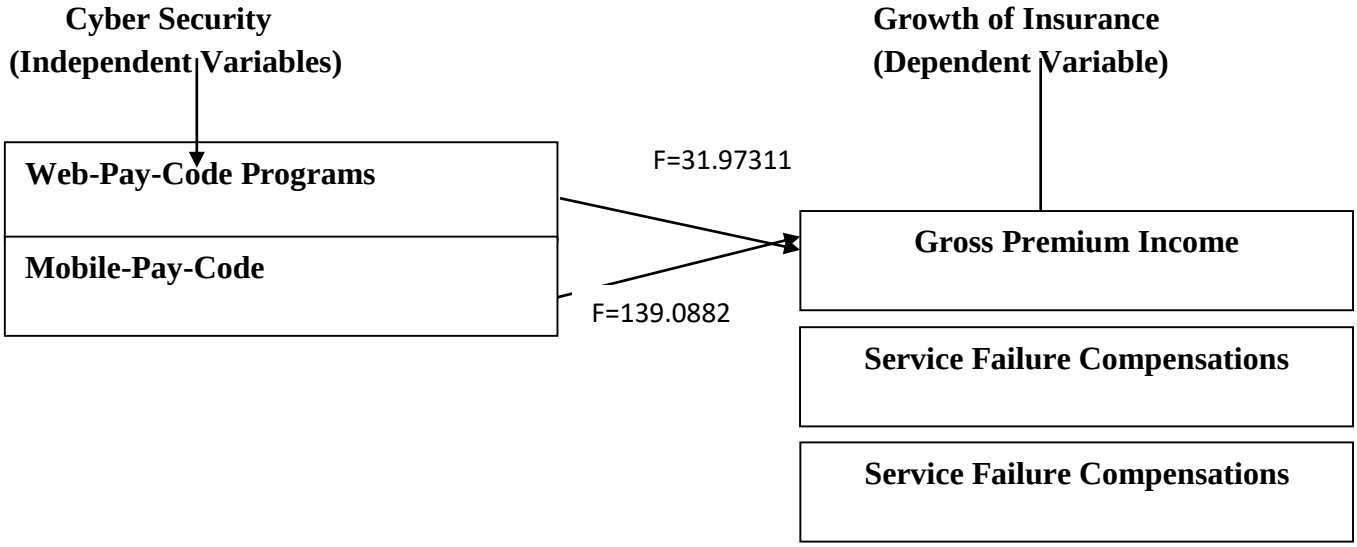

Figure 5.1: Researcher Own Model of Cyber Security and Growth of Insurance

REFERENCES

Anoke, A.F., Nzewi, H.N., Agagbo, O.C., & Onu, A.N.(2021). Micro insurance services and growth of women entrepreneurs in Onitsha, Anambra State, Nigeria. International Journal of Innovative Science and Research Technology, 6(8).507-513.

Abbas, G., & Shukur, I. (2021). The impact of training and development on job satisfaction: a case study of private banks in Erbil. International Journal of Social Sciences & Educational Studies, 2(1), 65-72

Abdulrahaman S. (2023). Bank loan and smes' performance in the Era of Covid 19

Ahmed, S & Afiouni, F. (2020). Human resource management and knowledge management: a road map towards improving organizational performance. Journal of American Academy of Business, Cambridge, 11(2), 124-134

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(1), 12-30.

Beck, T., Chen, T., Lin, C. & Song, F.M (2014). Financial innovation: the bright and the dark sides. Journal of Banking and Finance. 72 (2), 28-51

Bob-Alli, M.M (2010). Fundamentals of insurance operations, Barmco Publishers

Cengage (2019) Real–time monitoring and reporting. Available at: https://www.encyclopedia.com/environment/energy-government-and-defense- magazines/real-time-monitoring-and-reporting

Dalia, K.F (2022). SME competitiveness: the influence of the qualities of leadership on competitive advantage, International Journal of Language, Literature and Culture, 2(6), 1-20

Day, H & Daft, R. L. (2018). Management .6th Edition, South-Western West: Thomson

Dean, J., & Bowen, D. (2024). Management theory and total quality: improving research and practice through theory development. Academy of Management Review, 19(3), 392-418

Ebaye, A. S & Osim, T. A (2022). Utilization of Information resources and services among undergraduate students in federal university libraries in South-South, Nigeria, Texila International Journal of Academic Research, 1(2), 1-21

Faeq, D. K., Abdulla, D. F., Ali, B. J., & Akoi, S. (2021). Impact of job resources on employee green behavior: An Empirical Investigation among Employees Work in The Tourist Companies in Erbil-City Kurdistan Region of Iraq. The Scientific Journal of Cihan University– Sulaimaniya, 5(2), 115-126.

Flint, S (2020). Strategic leadership: top executives and their effects on organizations. New York: West Publishing Company, p. 6.

Flynn, B. B., Schroeder, R. G., & Sakakibara, S. (2024). A framework for quality management research and associated measurement instrument. Journal of Operations Management, 11(4), 339-366.

Gatzert, N., & Schubert, M. (2022). Cyber risk management in the US banking and insurance industry: A textual and empirical analysis of determinants and value. Journal of Risk and Insurance, 1(2), 56-89

Gambi, L. N. (2024). A influência da culture organizational no uso de técnicas da qualidade e seu impacto no desempenho (Tese de doutorado). Escola de Engenharia de São Carlos, Universidade de São Paulo, São Carlos

Hamisu, M.I (2020). Investigating the level and ways to improve resources utilization in federal polytechnics, International Journal of Social Science and Humanities, 8(3), 106-115

Heizer, M. A., & Ireland, D. (2022). The essence of strategic leadership: managing human and social capital, Journal of Leadership & Organizational Studies, 9(1), 3-14.

Hni-Ling, P, Gani M, Hamzah N & Rahman Z (2024). Effect of human capital and leadership on institutions performance and competitive advantages. International Journal of Management & Social Sciences, 7 (3): 479-488.

Huff, A. S., Floyd, S. W., Sherman, H. D & Terjesen, S. (2019). Strategic management. Logic and Action, John Wiley & Sons, New York

Hollnagel, E. (2017). Resilience–the challenge of the unstable. In resilience engineering (pp. 9-17). CRC Press

Ibegbulem, H. O. (2021). The language of indemnification and the economic growth of Nigeria: Perspectives from assurance firms. Linguistics and Culture Review, 5 (3), 41-54

John, J.I.T, Owui, S.M., Ndifon., H.O & Nkamare, S.E.I, (2024). The role of insurance industry on economic growth in Nigeria, Unicross Journal of Science and Technology, Ujost, 1(2), 117-125

Jorge, L.M.C., Carlos, M.P.H & Eduardo, M.R.R (2024). Influence of the logistics management system on the productivity of call centers, laccei international multiconference on entrepreneurship, innovation and regional development - LEIRD 2024, Journal of Business Management. Vol. 3 (8) 95 – 107

Klein, E. (2022). A concept analysis for strategic leadership. EBS Review No. 26(1), 37-57

Krslak, R.S., & Norton, D. P. (2021). The strategy-focused organization: how balanced scorecard companies thrive in the new business environment, Harvard Business Review Press, Boston, M

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

Li Y., & Liu Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports Journal. 7 (1), 8176-8186

Lompempe, B. G., Ndeba, L. C., Isaki, N. A., Mitungu, M. T., Boongo, M. D., Liyandja, I. H., Nswele, I. O., & Tshitadi, M. A. (2024). Experience of managers in the supply chain for medication and other pharmaceutical products. Health Economics and Management Review, 5(4), 19-32.

Mabonga, M.W. (2020). Financial bootstrapping strategy and sustainability of small and medium enterprises in Kanduyi Sub-County in Kenya. American International Journal, 1(2), 1-21

ManageEngine (2019) Real-time network monitoring. Available at: https://www.manageengine.com/network-monitoring/real-time-network-monitoring.html [Accessed on 21 April 2025]

Morgan, S.(2020). Cyber-crime to cost the world about ten point five (10.5) trillion dollars annually by 2025. Cyber warfare in the C-suit.

Oladipo, J. A. (2012). Information system and insurance business in Nigeria. JORIND, 10 (3):343-439.

Odeh, R. B. M., Obeidat, B. Y., Jaradat, M. O., & Alshurideh, M. T. (2019). The transformational leadership role in achieving organizational resilience through adaptive cultures: the case of Dubai service sector. International Journal of Productivity and Performance Management

Panda, A., & Bower, A. (2020). Cyber security and the disaster resilience framework. International Journal of Disaster Resilience in the Built Environment, 1(2), 12-45

Rouse M (2017) Real-time monitoring. Available at: https://whatis.techtarget.com/definition/real-time-monitoring [Accessed on 21 April 2025]

Seemma, P.S., Nandhini, S., & Sowmiya, M (2018). Over view of cyber security. International Journal of Advance Research in Computer and Communication Engineering.7 (11), 2-5

Srijana, P., & Fatta, B. K. (2017). Contribution of insurance in economic growth of Nepal. Journal of advanced academic research (JAAR), 4 (1), 99-110.

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Frame- work, standards and recommendations. Future generation computer systems, 92(1), 178-188

Sousa, R., & Voss, C. A. (2022). Quality management re-visited: a reflective review and agenda for future research. Journal of Operations Management, 20(1), 91- 109. http://dx.doi.org/10.1016/S0272-6963(01)00088-2

Stephens, J & Iskandaria, M. (2022). Study of entrepreneurial bootstrapping techniques. American society of engineering education.

Tariq, N. (2018). Impact of cyber attacks on financial institutions. Journal of Internet Banking and Commerce, 23(2), 1-11

Timi, F.B, Tolulope, O.A & Ismail, A.S (2023). Knowledge and practice of supply chain management of pharmaceuticals by health professionals in four States of South-South, Nigeria, Afr J Pharm Res Dev, 15(2), 91-100

Ujomudyke C.C., Dike G.N., Okeke C.O & Eboh O.S. (2024). Government policies and performance of pharmaceutical Firms in South-East, Nigeria, International Journal of Business and Management Review, 12(9), 85-118

Umar, I.(2019). The impact of cyber-crime on the Nigerian economy and banking system. Journal of Advanced Research in Computer Communication Engineering. 6(5), 318-329

Webb, L., Grace, M. F. & Skipper, H. (2005). The effect of banking and output. Journal of financial issues, 2(1), 1-21

Wu, H., Han, H., Wang, X., & Sun, S. (2020). Research on artificial intelligence enhancing internet of things security: A survey. Ieee Access, 8(1), 15-38

Wang, H.L (2024). Theories for competitive advantage, in hasan, h. (ed.), being practical with theory: a window into business research, wollongong, Australia: theory, Australia, 1(1), 33 – 43.

Zwane, B.K, & Nyide, C.Y (2022). Financial bootstrapping and the small sector in a pandemic in Kano State, Nigeria. Bayero Journal of Entrepreneurship Studies, 4 (2) 86 – 103