Effect of Cyber Securty Threat on the Performance of Insurance Industry 2002-2022: Nigerian Pespertive

Ugwu, Ndubuisi Christian[1], Okparaka, Vincent[2]
[1]*PhD Student, Department of Insurance and Risk Management, Enugu State University of science and Technology (ESUT).*
[2]*Ph. D HOD, Department of Insurance and Risk Management, Enugu State University of science and Technology (ESUT)*

***Abstract*—Cyber-security is of rules and regulations put in place for the protection and guiding of the cyber space in the world . Cyber-crime refers to the series of organized crime attacking both cyber space and cyber security. Cyber security has risen to become a national concern as threats concerning it now need to be taken more seriously. Cyber Security seeks to ensure the protection, availability and maintenance of the security features of the organization and to protect the user's property against related cyber security threats in the cyber environment. This study attempts to provide an overview of the effect of Cyber security threat on the performance of insurance Industry in Nigeria 2002-2022. Cyber-crime financial loss was use as the dependent variable, while total insurance asset and total insurance investment was used as the independent variables. Secondary data was used and sourced from Central Bank of Nigeria (CBN).The Ordinary Least Squares (OLS) were used to analyze the variables. The result of the findings shows that cyber security threat has negative and significant effect on the performance of insurance industry in Nigeria. Based on the findings, we recommend that technological measures such as Access control and "password security", Data's Authentication, Anti-virus software, Malware scanners, Firewall, should be put in place to prevent cyber security threat.**

I. INTRODUCTION

The world is becoming a global place and technology-based solutions are being adopted by organizations individual, companies, government and non-governmental organizations around the world, making the world a digital and globalize place. Based on this, the risk of cybercrime has increased and has continued to increase as the world grows, and this is especially true if the controls that are in place are insufficient or nonexistent. Incidents involving cyber risk can have a diverse range of effects on the businesses that are impacted by them the proper response lies in cyber security. Today more than 61% of full industry exchanges are done on the internet, so this area prerequisite high quality of security for direct and best exchanges. Thus, cyber security has become a most recent issue (Dervojeda, et. all., 2014
From business, industry, government to not-for-profit organizations, the internet has simplified business processes such as sorting, summarizing, coding, editing, customized and generic report generation in a real-time processing mode. However, it has also brought unintended consequences such as criminal activities, spamming, credit card frauds, ATM frauds, phishing, identity theft and a blossoming haven for cybercriminal miscreants to perpetrate their insidious acts. (Schaeffer, 2009)

Cyber-security can be described as a combination of methods, technologies and processes to protect the privacy, integrity and availability of computer systems, networks and data from cyber-attacks or unauthorized access. The main purpose of cyber security is to protect all institutional assets from both external and internal threats as well as barriers caused by natural disasters. Since organizational assets are made up of multiple different systems, effective and efficient cyber security consolidation requires coordinated efforts across all of its information systems. (Roseline, O. Moses-Òkè 2012)

The primary aim of cybercrime is to cause disruption in the cyber space to normal business operations as well as essential infrastructure with the intent of

committing fraud. Data that has been illegally obtained is frequently utilized by cybercriminals 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. The adversaries are currently employing more cutting-edge strategies in order to target the systems. Everyone from sole proprietors to multi-national corporations and everything in between is impacted. Because of this, each of these companies has realized the significance of maintaining a high level of cyber security and is actively working to put into place all of the preventative measures that are currently available to ward off potential cyberattacks, (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 cybersecurity. Better cybersecurity leads to increased consumer trust and income potential, but requirements for data protection and privacy are continually growing, making it more difficult to manage cybersecurity (Lee, 2021).

Managing risk associated with \cyber security involves many strategies, among them is limiting data access. This is done to avoid putting sensitive information at risk. Cybersecurity 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)

The purpose of this study was to determine the effect of Cyber Security threat on the Performance of Insurance Industry in Nigeria.

STATEMENT OF PROBLEM

The insurance companies activities are being threaten by the activates of cybercrime and this greatly affect the performance, profits and output of insurance industry in Nigerian. Nigerian cyber criminals are daily devising new ways of perpetrating this form of crime and the existing methods of tracking these criminals are no longer suitable for to deal with their new tricks. The Insurance companies as well show increasing naivety and gullibility at the prospects incited by these fraudsters.

Cyber-attacks have now become an unavoidable digital risk that even the most sophisticated financial institutions will never be able to completely eliminate cyber threats, no matter how much money they invest in cutting-edge protection technologies (Hausken, 2020). When a cyber-attack jeopardizes data availability, confidentiality, or integrity, it can trigger fear and cascading repercussions, resulting in poor insurance security performance. This will have an impact on stakeholders, so the insurance industry should adopt cyber security management techniques to address the issue of cyber-attacks.

Objectives of the Paper

The Broad objective of the study is to examine the effect of Cyber Security Threat on the Performance of insurance industry in Nigeria

While the specific objectives of the paper are:

1. to examine the impact of cyber crime on insurance investment , and
2. to access the effect of cyber crime on insurance assets in nigeria

The paper provides information about cyber security and cyber threat on the insurance performance. It covers various information about these topics in its subsections. Trends of cyber security and the role of security agencies in cyber security define in this paper. The paper provides some necessary information about cyber-crime.

II. LITERATURE REVIEW

2.1 Conceptual Review:

The issue of cyber-crime is one that has been discussed by many people with various perspectives on the issue, most coming at it from different sides than the others. Cyber-crimes have gone beyond conventional crimes and now have threatening ramifications to the national security of all countries,

even to technologically developed countries as the United States.

Professor Augustine Odinma (2020) states that "cyber-crime is any illegal acts perpetrated in, on or through the internet with the intent to cheat, defraud or cause the malfunction of a network device, which may include a computer, and other electronic devices. The illegal act may be targeted at a computer network or devices e.g., computer virus, denial of service attacks (DOS), malware (malicious code). The illegal act may be facilitated by computer network or devices with target independent of the computer network or device".

Overview of cyber-crime and cyber security

The technology has development have equally definitions of cyberspace, cyber security and cybercrimes. It has been argued that since computer crime may involve all categories of crime, a definition must emphasize the particularity, the knowledge or the use of computer technology. Cyber-space refers to the boundless space known as the internet. It refers to the interdependent network of information technology components that underpin many of our communications technologies in place today.

Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. (Wu et al., 2020)

Cyber security is the body of rules put in place for the protection of the cyber space. But as we become more dependent on cyberspace, we undoubtedly face new risks. Cyber-crime refers to the series of organized crime attacking both cyber space and cyber security. Sophisticated cyber criminals and nation-states, among others, present risks to our economy and national security. Nigeria's economic vitality and national security depend on a vast array of interdependent and critical networks, systems, services, and resources known as cyberspace. (Hausken, 2020)

Perhaps the most complete definition of Cyber-crime is as given "A criminal activity involving an information technology infrastructure, including illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (ID theft), and electronic fraud".

Goals of Cyber Security

The following are the objectives of Cyber-security.

- To help people reduce the vulnerability of their Information and Communication Technology (ICT) systems and networks.
- To help individuals and institutions develop and nurture a culture of cyber security.
- To work collaboratively with public, private and international entities to secure cyberspace.
- To help understand the current trends in IT/cybercrime, and develop effective solutions.
- Integrity, which may include authenticity and non-repudiation.
- Confidentiality.

Categories of Cyber Crime

Hacking: Hackers make use of the weaknesses and loop holes in operating systems to destroy data and steal important information from victim's computer. It is normally done through the use of a backdoor program installed on your machine. A lot of hackers also try to gain access to resources through the use of password hacking software. Hackers can also monitor what u do on your computer and can also import files on your computer. A hacker could install several

programs on to your system without your knowledge. Such programs could also be used to steal personal information such as passwords and credit card information. Important data of a company can also be hacked to get the secret information of the future plans of the company.

Cyber-Theft: Cyber-Theft is the use of computers and communication systems to steal information in electronic format. Hackers crack into the systems of banks and transfer money into their own bank accounts. This is a major concern, as larger amounts of money can be stolen and illegally transferred. Credit card fraud is also very common. Most of the companies and banks don't reveal that they have been the victims of cyber -theft because of the fear of losing customers and shareholders. (Hua,J & Bapna, S 2013)

Viruses and worms is a very major threat to normal users and companies. Viruses are computer programs that are designed to damage computers. It is named virus because it spreads from one computer to another like a biological virus. A virus must be attached to some other program or documents through which it enters the computer. A worm usually exploits loop holes in soft wares or the operating system.

Spamming– involves mass amounts of email being sent in order to promote and advertise products and websites. Email spam is becoming a serious issue amongst businesses, due to the cost overhead it causes not only in regards to bandwidth consumption but also to the amount of time spent downloading/ eliminating spam mail. Spammers are also devising increasingly advanced techniques to avoid spam filters, such as permutation of the emails contents and use of imagery that cannot be detected by spam filters.

Financial Fraud- These are commonly called "Phishing' scams, involves a level of social engineering as they require the perpetrators to pose as a trustworthy representative of an organization, masquerades as a legitimate business or reputable person.

Identity Theft, Credit Card Theft, Fraudulent Electronic Mails (Phishing): Phishing is an act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in order to scam the user into surrendering private information that will be used for identity theft.

Cyber harassment- is electronically and intentionally carrying out threatening acts against individuals. Such acts include cyber-stalking.

Cyber laundering- is an electronic transfer of illegally-obtained monies with the goal of hiding its source and possibly its destination.

Website Cloning: One recent trend in cyber-crime is the emergence of fake 'copy-cat' web sites that take advantage of consumers who are unfamiliar with the Internet or who do not know the exact web address of the legitimate company that they wish to visit. The consumer, believing that they are entering credit details in order to purchase goods from the intended company, instead unwittingly entering details into a fraudster's personal database. The fraudster is then able to make use of this information at a later stage, either for his own purposes or to sell on to others interested in perpetrating credit card fraud.

Insurance Companies

First of all, let us discuss risk because is an aspect of insurance, however, being a phenomenon that entangled with various disciplines has made it difficult for scholars to arrive at a consensus definition of the concept as every attempt tends to derive a different perceptive narrowed and peculiar to that particular discipline. As defined by Oyetayo (2016), the risk is a possibility of adverse deviation from the desired outcome that is hoped for.

Also, Sanusi (2019) defined risk to be the probability that an organization or individual will not be able to meet some expectations it has set in a given period. Elogu (2017) defined risk to be the combination of the probability of an event and its consequences. For the sake of this study, the above definition by Elogu (2017) will be adopted as it gave a clear view of the prevalent issues of uncertainty which tends to be unavoidable in every aspect of life, given the need to formulate the concept of insurance to aid in

cushioning the negative effect of such unforeseen contingencies.
Apart from risk management, the insurance sector is known to be huge investors in other vibrate economic activities.

Measuring insurance asset has been the major attribute in understanding the performance of the insurance sector. In quantifying growth in the sector, variables such as insurance penetration, total premium, total insurance income, and insurance density have been prevalent. The penetration rate is measured as the ratio of premium underwritten in a particular year to the gross domestic product of the same year. Elogu (2017) defined insurance penetration as a product's sales volume relative to the sales volume of competing products. Within insurance, there is life insurance penetration which considers premium from life insurance policies only as a percentage of GDP, and non-life insurance penetration which considers premium from other than life insurance policies like auto insurance, health insurance, business insurance, etc.

Insurance Market Operation
Insurance Market Operation is the buying and selling of insurance and the entities involved in these transactions (Acharya, 2015).
Insurance Market Operation is described as the process technologies and human resources, that allows marketing insurance product to scale (Utomi, 2016).

Omer (2016) states thatInsurance Market Operation is how insurance business is been carried out by providing financial protection against potential risk and losses to individuals or businesses.

Asset of Insurance Companies
Most times insurance asset is measured with consolidated insurance total asset across Nigeria. Magoulios (2016) refers insurance asset as totality of the cost of economy involved in the purchase of new plants and machinery with the aim of increasing the stocks of raw materials and products for new homes as investment on a macroeconomic Level. Assets are resources controlled by an entity as a result of past events and from which future economic benefits or service potential are expected to flow to the entity. Asset also refers to an items or properties owned by persons or company, which have value and available to meet debts and commitments. Assets are useful or valuable resources owned by a firm, these are normally split into current assets and non-current (Long term) assets.

Sullivan and Sheffrin (2018) define assets as anything tangible or intangible that can be owned or controlled to produce value and that is held by a company to produce positive economic value. Simply stated, assets represent value of ownership that can be converted into cash (although cash itself is also considered an asset. The balance sheet of a firm records the monetary value of the assets owned by that firm. It covers money and other valuables belonging to an individual or to a business. Basically, we have two types of assets namely current assets and non-current assets.

2.2 Empirical Review
Abdulrahim (2019) researched on "the managing cybersecurity as a business risk in small and medium-sized enterprises that are focused on information technology". The objectives of the research was to identify the most significant cybersecurity threats that Kenyan small and medium-sized enterprises (SMEs) are currently facing and to devise an implementation strategy that will provide a road map for the management of cyber-risk as a business risk.
Research that was conducted included both quantitative and qualitative methods. In order to perform an analysis on the obtained quantitative data, it was first given a numerical classification. In order to make analysis easier, the qualitative data that was gathered from primary sources was arranged in a methodical fashion. The findings of the research indicate that cyber security investments, cyber security management, training and awareness, cyber security policy programs, cyber security vulnerability management programs, real-time network monitoring, and incident management all play a significant role in the management of cyber-risk within SMEs.

Cyber fraud and the risks Associated with Insurance Performance
Gatzert and Schubert, (2022) carried out a textual and empirical investigation into the management of cyber

risk in the banking and insurance industries in the United States. The objective of the study is to asctain the effect of cyber crime on the banking and insurance firms. Their findings indicate that businesses across all sectors are becoming more aware of the dangers posed by cyber-attacks. In addition, they find that across the entire sample, companies belonging to the banking industry that have a higher cyber risk consciousness score as well as a higher general risk awareness are more likely to implement cyber risk management.

Umoren & Emen (2016) investigated the relative contributions of the Insurance Industry to the growth of the Nigerian economy within the period of 1970 to 2012. Multiple linear regression method was used to test the research hypothesis. Their result showed that the Insurance sector growth has contributed significantly to the economic growth in Nigeria within the period under review; however, the claim expenditure has a negative influence on GDP growth. They are of the opinion that claim administrators should be trained in claims reporting process like, investigation, verification of claims, loss minimization and evaluation. This will help to reduce the frequency of claim notification and increase premium income for economic development and growth.

Cyber Crime and Insurance Investments

Jegede and Olowookere (2016) carried out research on the prevalence of cyber fraud and the risks it poses to business environments in Nigeria. The participants of the study were the various financial institutions that are located in Nigeria. According to the findings, detected risks need to be properly addressed in order to prevent secondary impacts that lead to vulnerabilities that interfere with the life of the institution as well as the well-being of its customers. Institutions have an additional responsibility beyond the installation of threat response technologies: they must work to strengthen the trust environment. They have a responsibility to their customers to keep them informed about the existence of actual and potential risks posed by the online environment. In order to avoid the compromise of personal information that is vital to the clients' financial and domestic survival, protective actions need to be implemented, and obtaining clients' consent is essential in this regard, particularly when such requests are made for secondary uses of the information

III. METHODOLOGY

3.1 Data and Sources

To capture the effect of cyber security threat on Insurance Industry performance, cybercrime financial loss (CYBER) is used as proxy for Cyber security threat as the Dependent Variable; While Total Insurance Investment (INSIV) and Total Insurance Asset (INSA) as independent variables which are the measures of Insurance Performance act as the major explanatory variables in the model. The disturbance variables not specified in the model is being captured by the stochastic error term. Before the variables were included in the model they were tested for stability and cointegration. The variables where sourced from the statistical bulletin of the Central Bank of Nigeria, 2022 and the National Bureau of Statistics.

3.2 Model Specification

General form of OLS model with n lags for variable Y and m lag for variable X is as follow:

$$CYBER_t = \beta 0 + \beta_1 INSIV_t + \beta_2 INSA_t + \mu_t \quad (2)$$

Where

$CYBER_t$ = Real Gross Domestic Product

$INSIV_t$ = Total insurance Investment

$INSA_t$ = Total insurance Asset

β_0 = Center of origin

β_1- β_2 = Coefficient of estimate

U_t = Error term

3.3 Description of Variables

3.3.1. Dependent variable

The dependent variable is the Cyber Security Threat

Independent variables

The independent variable are made up of the total investment of insurance and insurance Assets in Nigeria.

Insurance investment is the total amount of money invested by the insurance company in various assets. The amount invested is usually derived from the proportion of the total premium.

Insurance Asset is adopted as a measure of the insurance sectors development indicator (Islam and

Osman, 2011).. Financial assets for the insurance industry include a totality investment in government securities as well as stocks & bonds. This measure is referred to as the measure of size of the sector relative to the size of the economy. It indicates a larger insurance sector development and therefore greater intermediation activities and vice versa.

IV. DATA PRESENTATION AND ANALYSIS

Transformed Log of the Data

	LNCYBER	LNINSA	LNINSIV
2002	8.72648119...	11.3534106...	10.5170738...
2003	9.57387175...	11.7301907...	10.9085734...
2004	8.90422273...	11.8580886...	11.2197717...
2005	9.93051889...	12.2215183...	11.7104986...
2006	10.0358745...	12.6363689...	12.2846985...
2007	10.2181887...	12.9657029...	12.7045663...
2008	10.2982286...	13.2589105...	12.7263278...
2009	11.0654970...	13.2818589...	12.7480893...
2010	10.9719670...	13.2793941...	12.7698508...
2011	10.9319634...	13.3392395...	12.7916122...
2012	11.0104317...	6.37398356...	10.3783938...
2013	11.3968522...	6.15038952...	10.5170738...
2014	11.4221689...	6.54985100...	10.9085734...
2015	11.7406266...	6.68824262...	11.2197717...
2016	9.75458142...	6.91351863...	11.7104986...
2017	11.9817846...	7.05763972...	12.2846985...
2018	12.6385658...	7.14001713...	12.7045663...
2019	12.8980766...	7.38798766...	12.7263278...
2020	13.0803990...	7.60964909...	12.7480893...
2021	13.5768357...	7.38798766...	12.7698508...
2022	13.9774584...	7.60964909...	12.7916122...

Summary of Unit Roots Test Results

Variables	PP Statistic	Critical Value @ 5%	Probability Value	Stationary
LNCYBER	-3.4442	-3.6584	0.0737	I(0)trend & intersect
LNINSIV	-3.4940	-3.6736	0.0684	I(1)trend & intersect
LNINSA	-3.9355	-3.6736	0.0310	I(1)trend & intersect

Source: Author's E-view 12.0 calculations

From the result of Philip and Peron unit root, statistics shown in table, indicates that all the variables log of Cybercrime financial loss, log of insurance investment and log of insurance assets are all integrated at order one I(1) and 1(0), thereby chosen the best model called ordinary least square.

Normality Distribution

The statistical property of the data sets are seen as vital determinants of their behavior when used in econometric analysis. On the basis of this, the researcher presented, the basic descriptive statistics called normally test of the variables under study.

	LNINSA	LNCYBER	LNINSIV
Mean	9.656838	11.14927	11.95907
Median	7.609649	11.01043	12.28470
Maximum	13.33924	13.97746	12.79161
Minimum	6.150390	8.726481	10.37839
Std. Dev.	2.933059	1.480442	0.909068
Skewness	0.135115	0.265396	-0.552423
Kurtosis	1.176146	2.211277	1.680790
Jarque-Bera	2.974533	0.790846	2.590876
Probability	0.225990	0.673395	0.273778
Sum	202.7936	234.1346	251.1405
Sum Sq. Dev.	172.0567	43.83418	16.52808
Observations	21	21	21

Source: Author's E-view 12 calculation

Decision Rule:
For a variable to be normally distributed, the variable must be trending towards the Jargue-Bere statistics. The Skewness and Kurtosis must be relevant.
Table above contains the basic measures of central tendency, spread and variation calculated on the different serials of the data set. The mean of the distribution measures aggregating tendency of the data. Hence, the mean of LNCYBER is 11.14, while that of LNINSIV, LNINSA are 11.95907, and 9.6569 respectively. the median measures the spread of the variable in the distribution. Hence, the median of LNCYBER is 11.0104 while that of LNINSIV, LNINSA are 12.2847, and 7.6096 respectively.
Finally, all the variables are normally distributed because they are tending towards 3. However, since other variables are normally distributed. There is no variable to disrupt the normality distribution of the variable for the study

REGRESSION RESULT

Dependent Variable: LNCYBER
Method: Least Squares
Date: 07/28/24 Time: 13:07
Sample: 2002 2022
Included observations: 21

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	13.23242	0.452862	29.21952	0.0000
LNINSA	-0.394539	0.045559	-8.659963	0.0000
INSIV	8.09E-06	9.79E-07	8.266311	0.0000

R-squared	0.863336	Mean dependent var	11.14927
Adjusted R-squared	0.848151	S.D. dependent var	1.480442
S.E. of regression	0.576895	Akaike info criterion	1.869251
Sum squared resid	5.990541	Schwarz criterion	2.018468
Log likelihood	-16.62713	Hannan-Quinn criter.	1.901635
F-statistic	56.85509	Durbin-Watson stat	1.874705
Prob(F-statistic)	0.000000		

V. RESULT AND CONCLUSION

The result reveals that cyber security threat had a negative and significant effect on the performance of insurance industry in Nigeria. This means that the performance of insurance industry are being effected by the activities of cybercrime. The explain variation is very high and good for the interpretation of any of econometric result.

VI. CONCLUSION

It is observed that the Assets of the Insurance Industry and insurance investments which are the measures of insurance Performance is negatively affected by the increase in cybercrimes. This corresponded with existing a priori expectation which states that increase in cyber security threat will lead to Decrease in the performance of insurance industry in Nigeria. This implies that as Insurance companies are victims of cyber attracks, it will have more negative impact on the performance of insurance industry. On the other hand, decrease in the cyber-attacks on the insurance business will have a positive effect on the performance of insurance industry. It also conform to a priori expectation, which states that an increase in cyber security will lead to decrease in cyber-attacks. The economic implication of this findings is that although investing in cyber security will affect the finances of the Insurance companies, but it will impact positively on the performance of insurance Industry.

VII. RECOMMENDATION

Based on the findings and conclusions, it was recommended that

The insurance industry and government should put proper mechanism in place to prevent its investment and assets from cyber attacks

REFERENCE

[1] Adeyele.J.S. (2011), Economic liberation of insurance industry in Nigeria. International Journal of Research in Management, 2(1).

[2] Afees, A. S., &Ajide, B. K. (2016).The Stock Market and Economic Growth in Nigeria: An **Empirical Investigation. Journal of Economics** Theory, 4(2), 65-70.

[3] Akinlo.T. (2014) The Causal relationship between Insurance and economic growth in Nigeria (1986 – 2010). Australian journal of Business and management, 4(5)

[4] Dickey, D. A. & Fuller W. A. (1979). Distribution of the Estimation for Autoregressive Time Series with a Unit Root. Journal of the American Statistical Association.

[5] Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. Procedia Economics and Finance, 24-31. doi:10.1016/S2212-5671(15)01077-

[6] Cabaj, K., Kotulski, Z., Księżopolski, B., & Mazurczyk, W. (2018). Cybersecurity: trends, issues, and challenges. EURASIP Journal on Information Security. doi:10.1186/s13635- 018-0080-0

[7] Fadun, O. S. & Shoyemi, O. S. (2018) Insurance investment funds and economic growth in Nigeria: An empirical analysis (2000-2015), International Journal of Development and Management Review, 13(1), 73-88

[8] Hidayat, I. P., & Firmansyah, I. (2017). Determinants of financial performance in the Indonesian Islamic Insurance Industry. Etikonomi, 16(1), 1–12.

[9] Gross, M. L., Canetti, D., & Vashdi, D. R. (2017). Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. Journal of Cybersecurity, 3(1), 49–58. doi:10.1093/cybsec/tyw018

[10] Hua, J., & Bapna, S. (2013). The economic impact of cyber terrorism. The Journal of Strategic Information Systems, 22(2), pp. 175-186.

[11] Kanbiro, O.D. & Ayneshet, A. A. (2019). Factors affecting financial performance of insurance companies operating in Hawssa city Administration, Ethiopia, 2008-2018. Universal Journal of Accounting and Finance, 7(1) 1-10.

[12] Kumar, S., & Somani, V. (2018). Social Media Security Risks, Cyber Threats And Risks Prevention And Mitigation Techniques. International Journal of Advance Research in Computer Science and Management, 4(4), pp. 125-129.

[13] Panchanatham, D. N. (2015). A case study on Cyber Security in E-Governance. International Research Journal of Engineering and Technology.

[14] Okonkwo, O., Ogwuru, H. & Ajudua, E. (2018). Stock market performance and economic growth in Nigeria: An Empirical Appraisal. European Journal of Business and Management 6 (26) 33 – 42

[15] Olumide, O. O.,Victor, F. B. (2010): E-Crime in Nigeria: Trends, Tricks, and Treatment. The Pacific Journal of Science and Technology, Volume 11. Number 1. May 2010 (Spring)

[16] Oyetayo, Y. (2016). Towards effective risk management in the insurance industry: A review of the Nigeria situation. Institute of Advance Scholars (IAS) Publication, 7(14), 3-35

[17] Roseline, O. Moses-Òkè (2012): Cyber Capacity Without Cyber Security: A Case Study OfNigeria‟s National Policy For Information Technology (NPFIT), The Journal Of Philosophy, Science & Law Volume 12, May 30, 2012, Retrieved from www.Miami.Edu/Ethics/Jpsl

[18] Schaeffer, B. S., et al. (2009): Cyber Crime And Cyber Security: A White Paper For Franchisors, Licensors, and Others

[19] Yaqub, J.O & olagide,V.O (2010). Exchange rate changes and output performance in Nigeria: A sectorial analysis, Pakistan Journal of Social Sciences, 7 (5), 380-387.