The Impact of Cyber-Crimes on Depositors Accounts in Some Selected Deposit Money Banks in Kaduna State, Nigeria

Alhaji Kawugana PhD,[1] Shuaibu Said Abdullahi,[2] Ayanwuyi Johnson[3]
Federal Polytechnic Bauchi.
Dass Road Opp Gwallameji[1]Cavendish University Uganda[2]
P.M.B.0231 Bauchi, Bauchi State Nigeria
alhajikawugana@gmail.com[1]shuaibusaid01@gmail.com[2],johngreat70@gmail.com

DOI: 10.56201/ijbfr.v10.no4.2024.pg68.81

Abstract
This study examines the impact of cyber-crimes on depositors' accounts in some selected deposit money banks in Kaduna State, Nigeria. In Nigeria today, several internet crimes known as cyber-crimes are committed or perpetrated on daily basis and in various forms such as electronic spam mails, identity theft, hacking, BVN Scam, Web Jacking, cyber stalking, phishing among others. Cybercrime is a threat against various individuals/institutions and people, most especially depositors who are connected to the internet for their daily transactions. The objective of this study is to examine the impact of cybercrimes on depositor's account of some selected Deposit Money Banks. To achieve this objective, three (3) research questions and two hypotheses were formulated; Data were collected from both primary and secondary source judgmental sampling method was used to select some deposit money banks customers , out of the 206 questionnaires distributed, 200 questionnaires were utilized, while descriptive statistics, correlation matrix and panel data analysis (Random-effect GLS regression techniques) were utilized as analytical tools in the study with the aid of Statistical Package for Social Sciences (SPSS).To analyse the data obtained, frequency and simple percentage and regression analysis was used. This study reveals that different types of cyber-crimes have an impact on depositor's accounts and on Nigerian banking industry and it has have a negative impact on online banking transactions. The impact of this kind of crime can be felt on the lives, economy and international reputation of a nation. Hence, the study concludes that there is a high level of banking cybercrime activities in Kaduna state, banks online protocols against banking cybercrime activities in Kaduna is adequate, Fight against banking cybercrimes in Kaduna by the related agencies is below expectation, poor Financial literacy and low knowledge of internet operation are the major causes of banking cybercrimes in Kaduna and the awareness creation on banking cybercrimes by all the related agencies are adequate therefore the study recommend that there should be more awareness creation on banking cybercrimes by all the related agencies to reduce the rate of online banking transactions and other types of cybercrimes in Kaduna. Also Depositor's should be able to identify, authorized and reputable web sites, where they can make their day-to-day transactions, and only supply their bank information's to secured sites, and their deposit money banks when they need arise if they must make transactions online, and should report to their local banks if there is any suspect of leak of information

Keywords: *Cybercrime, Deposit Money Banks, Depositors Account, Internet*

INTRODUCTION

The term cybercrime can be used to describe any criminal activity which involves the use of computer or the internet network (Okeshola, 2013). This term is used for crimes such as fraud, theft, blackmail, forgery, and embezzlement, in which computers or networks are used. Cyber-crime is believed to have started in the 1960's in the form of hacking. This was followed by privacy violations, telephone tapping, trespassing and distribution of illegal materials in the 1970s.In (Maitanmi, 2013) cybercrime was defined as a type of crime committed by criminals who make use of a computer as a tool and the internet as a connection in order to reach a variety of objectives such as illegal downloading of music files and films, piracy, spam mailing, duping depositors and the likes. Cyber-crime evolves from the wrong application or abuse of inter-net services. The concept of cybercrime is historical. It was discovered that the first published report of cybercrime occurred on the mainframe computer in the 1960s (Maitanmi, 2013). Since these computers were not connected to the internet or with other computers, the crime was committed by the employers (insider) in the company, hence it was referred to as computer crime rather than cybercrime.

Banking activities have become more complex with the introduction of Information and Communication Technology (ICT), which has changed the mode of bank crimes and fraudulent practices. Berney (2008) discovered that customers highly depend on the internet for their banking activities, which has led to an increase in the activities of online banking transactions. Gates and Jacob (2009) and Malphrus (2009) opined that the internet and online banking provides cybercrime with great opportunities to attack bank customers who are not physically present on the internet to confirm their online banking transactions.

Okpara (2009) revealed that one of the factors that impacted the most on the banking system's performance in Nigeria was fraudulent practices. Since the fraudulence in banks has become an ever-existing problem. It is evident from their study that, the internet constitutes the larger channel through which cybercrimes were perpetrated in banks in 2016. On this backdrop, Gartner (2019) predicted that worldwide spending on information security will significantly grow to $124 billion in 2019. And still, spending according to some security researchers estimate that cybercrime costs will quadruple from their figure in 2015 to about $2.1 trillion by end2019, and outpace expenditure on cyber-security by over 16 times. The vulnerability of this electronic market to criminal activities has therefore been a growing concern. Nigeria's internet penetration since the 21st century had been on the increase. Internet users as a percentage of the population increased significantly from 3.5% in 2005 to 47.4% in 2014 (WDI, 2016). Similarly, tele density has been forecasted to continuously increase overtime in Nigeria (Asemota, et al, 2015). The proliferation of the internet in Nigeria has indeed come with an unintended consequence, as a haven for criminals. Cybercrime has remained a challenging issue despite increasing awareness and attention to addressing the menace in Nigeria and across the globe. For instance, Cybercrime accounted for about 43% of total monetary loss due to fraud in 2016. As observed by AbdulRaheem, Isiaka, and Muhammed (2012), the degree and incidence of cybercrime in the Nigerian banking industry have been on the increase with obvious implications on bank performance such that it has a negative social impact

on the banking sector. Cybercrime is a new trend that is gradually growing as the internet continues to penetrate every sector of our society and no one can predict its future. The crime usually requires a hectic task to trace. Generally, cybercrime may be divided into one of two types of categories; Crimes that affects computer networks and devices directly. Examples are malicious code, computing viruses and malware etc. or Crimes facilitated by computer networks or devices, the primary target of which is independent of the computer networks or device. Examples include Cyber Stalking, Fraud and identity theft, phishing scams and information warfare.

There are few innovations that have changed the dynamics of banking as much as the e-banking revolution. Throughout the world, banks are reorganizing their business strategies to take advantage of new business opportunities offered by e-banking. Electronic banking is believed to have started in the early 1980s It has since then been growing in an unprecedented dimension in line with the growth in ICT development. E-banking has enabled banks to overcome borders, adopt strategic outlook, and bring in new possibilities. According to (Nitsure), information communication technology has reduced the cost of processing and facilitating the transmission of information leading to drastic changes in the banking business. The E-banking system has also make it very easy for depositors to carry out numerous transactions across the internet and provides easy access and movement of funds to make payment, settle debt or in performing other services. This research work examines what cyber-crime is, the different types of cyber-crimes that exist and their impact on bank depositors, impact and aspects of modern life and business.

Statement of the Research Problem

Advancements in information and communication technology (ICT) have redefined the ways banks carry out their businesses and turned the whole world into a global village. However, it has brought about numerous problems accompanying such great benefits. Nefarious software continues to be developed on a daily basis and circulated, fraudsters are now common everywhere around the world. Vast amount of database is subsequently destroyed and lost to these vile. More so, computer hackers and crackers hack into restricted database and commit fraudulent activities using their computer skills. Large amount of bank deposits is stolen/lost making some depositors lose faith and do away with banking system. Thus, making banking operations very difficult and stressful.

The larger society expects greater accountability, fairness, transparency and effective intermediation from banks, ensuring that they carry out their responsibilities with sincerity of purpose and unquestionable integrity with respect to their operations as a means towards earning public trust and goodwill. The banking business has become more complex with the development in the field of Information and Communication Technology (ICT) which has changed the nature of bank fraud and fraudulent practices. Berney (2008) observed that customers rely heavily on the web for their banking business which leads to an increase in the number of online transactions. Gates, Jacob and Malphrus (2009) assert that the internet provides fraudsters with more opportunities to attack customers who are not physically present on the web to authenticate transactions.

In Nigeria, in spite of the banking regulation and bank examination by the Central Bank of Nigeria (CBN), the supervisory role of the Nigeria Deposit Insurance Corporation (NDIC), and The Chartered Institute of Bankers of Nigeria (CIBN), there is still a growing concern about cyber-

crime fraud and other unethical practices which concerns the banking industry. Okpara (2009) found that one of the factors that impacted the most on the performance of the banking system in Nigeria was fraudulent practices. The research intends to enlighten the impact of cyber-crimes on depositors account in some selected deposit money bank in Kaduna Sate Nigeria as a GAP to fill

Objectives of the Study

The main objective of this research work is to examine the impacts of cyber-crime on depositor's accounts in some selected deposit money banks in Kaduna State Nigeria.
The specific objectives are to:

1. To identify and distinguish different types of cyber-crimes.
2. To examine the impact of cyber-crimes on depositors' Accounts
3. To examine the impact of cyber-crime laws in preventing cyber-crimes on depositor's account.

Research Questions

1. What impact does different types of Cyber-crimes have on depositors and on Nigerian banking industry?
2. To what extent does cyber-crime have on the level of trust the depositors have on their deposits with the bank?
3. What effect does government laws and regulations have in curbing or mitigating cyber-crime cases in Nigeria?

Scope of the Study

The objective of this research is to examine the impact of cyber-crimes on depositors account in some selected deposit money banks in Nigeria, and the research is limited to some selected bank depositors in some selected deposit money banks in Kaduna State.

Hypothesis

H_1 Cybercrimes have a negative impact on online banking transactions by bank customers in Kaduna

H_0 Cybercrimes have no negative impact on online banking transactions by bank customers in Kaduna

Literature Review

Conceptual Framework

Cybercrime is also defined as a crime in which a computer is the object of the crime or is used as a tool to commit an offense. Cybercriminals may use computer technology to access personal information, business trade secrets or use the internet for exploitative or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers. Cybercrime may also be referred to as computer crime.

Cyber-crime may also be referred to as any form of misconduct in cyber space. It is simply defined as the criminal use of the Internet. Cyber-crime is believed to have started in the 1960's in the form of hacking. This was followed by privacy violations, telephone tapping, trespassing and distribution of illegal materials in the 1970s. The 1980s witnessed the introduction of viruses. The

fast pace of development of ICT from the 1990s till today has added to the list of criminal exploits in cyber space. Today, the Internet is used for espionage and as a medium to commit terrorism and transnational crimes. With e-banking gaining ground in Nigeria, customers and online buyers are facing great risk of unknowingly passing on their information to fraudsters. "Hackers" get information of those who have made purchases through websites and then make fake cards, which they use with less detection.

The definition of cybercrime as a concept has been a major issue with different scholars. However, this study reviewed some definitions by some selected scholars. Cybercrime is seen as computer crime, computer-related crime, digital crime, information technology crime (Maat, 2004) and cybercrime could reasonably include a wide difference in criminal activities. In the 10th conference on Prevention of Crime and Treatment of Offenders, a conference dedicated to the activities on crimes related to computer networks which were carried out by United Nations Congress, cybercrime activity was subdivided into two definitions. Firstly, Cybercrime in a narrow sense of definition is an illegal activity directed by the process of electronic operations that are targeted towards the security of computer systems and the data processed by them. Secondly, cybercrime in a broader sense of definition is an illegal activity done utilizing, or about, a computer system, which includes crimes as illegal possession and offering or distributing information using a computer system (United Nations, 2005).

Empirical Review

Viraja and Purandare (2021) embarked on a qualitative research on the impact and challenges of cybercrimes. They administered qualitative questionnaires to 110 respondents of different age groups and gender then applied qualitative data analysis of grounded theory. They concluded that with the increasing rate of technology, cybercrimes can render even the entire government of a country bankrupt.

There have been an extensive studies conducted in many countries on cyber-crimes and its effect on banking activities, for instance; J.A. Mshana (2020) carried out a comprehensive report on " The impact of cybercrime on society". He employed the use of survey using questionnaires which was distributed to 250 people out of which 200 people responded and also took interviews. The total respondents were 80% out of the whole 250. He came to a conclusion that the impact of cybercrime has become unsustainable, considering the global economic crisis.

There are several empirical studies on cybercrime, banking systems, and related literature, but for this study, selected studies on cybercrime and banking system were reviewed; among them is the work of Akinfala (2005) researched job involvement/ experience factors and fraudulent behaviors among serving and convicted bank staff. The study found that job involvement has three factors: motivation, identification, and a feeling of pride that people achieve in their jobs. Nwude (2006) carried out a bank fraud using the methodology of interaction with bank staff of various cadres with a structured questionnaire to identify the fraud forms and characteristics in the banking industry. The study reveals that some staff involved in fraud due to greediness and arrogance

Cybercrime according to Douglas and Loader (2000) can be defined computer mediated activities conducted through global electronic networks which are either illegal or considered illicit by certain parties. In the banking sector, the cybercrimes which are committed using online

technologies to illegally remove or transfer money to different account are tagged as banking frauds (Wall, 2001).

The cybercrimes according to Wall (2001) can be categorized into four major categories i.e. cyber deceptions, cyber-pornography, cyber-violence and cyber-trespass. The banking frauds are sub-categorized in cyber-deception which can be defines as an immoral activities including stealing, credit card fraud, and intellectual property violations (Anderson et al., 2012).

There are number of frauds or cybercrimes witnessed in the banking sector, like ATM frauds, Cyber Money Laundering and Credit Card Frauds. However, in general all the cyber-crimes and frauds are executed with the ultimate goal of gaining access to user's bank account, steal funds and transfer it to some other bank account. In some cases, the cyber criminals use the banking credentials like PIN, password, certificates, etc. to access accounts and steal meager amount of money; whereas in other cases they may want to steal all the money and transfer the funds into mule accounts. Sometimes, the intention of cybercriminals is to just harm the image of the bank and therefore, they block the bank servers so that the clients are unable to access their accounts (Hutchinson& Warren, 2003).

Another study done by Hannan& Blundell (2004) on the issue relating to electronic crime and how it's not the only concept to be worried about. Their study focused mainly on two case studies, one of the study was to do an analysis of the important and crucial factors affecting the breakdown of electronic criminal activities in Australia. The other part of the study tried to address the costs that are incurred under the legal environment of the banks. The study found out that there are many consequences and costs that banks face from poor implementation of legal requirements and security measures. The study presented a number of options and solutions required in tackling policy strategies for future development.

Raghavan&Parthiban (2014) focused on the effect of cybercrime on bank finances. The main objective of their study was to discuss the problem of cybercrime in the banking sector. The study did an in-depth analysis of criminal activities and scenarios within the networks and identified the actors involved in each scenario. The study also identified and documented the various types of criminal activities that are plaguing the banking sector and the motives behind those who commit such crimes. This study identified that one of the costs emanating from such vice is the financial loss which represents a direct cost and a huge issue globally impeding the development of systems.

According to Moore, Clayton & Anderson (2009) they did a paper on the economics of online crime. According to their study, online criminal activities take place as a result of a number of idle nuisance hackers. The paper identifies that the banking institutions face a lot of problems trying to control their exposure to operational risks arising from network connections. Their study found that there are significant techniques and improvements that are viable in dealing with online crimes. The institutions must incur security costs for this to take full effect.The study suggested that in order to tackle online crime the banks must first understand the economic perspective.

In another study in Nigeria, Onuorah and Ebimobowei (2011) investigated the fraudulent activities and forensic accounting in Nigeria. The research revealed a need for banks in Nigeria to adopt more proactive measures such as forensic accounting procedures in the bank system. The study of Abdulrasheed, Babaitu, and Yinusa (2012) examined the impact of fraud on Nigeria's bank performance. The study results show a significant relationship between banks' profit and the total amount of funds involved in fraud. Also, a study done by Kanu and Okorafor (2013) researched

the nature, extent, and economic impact of fraud on bank deposits in Nigeria using descriptive and inference statistics. The study examined a positive significant relationship between bank deposit and fraud in the Nigerian banking industry. Iyodo, Agbaji, and Abu (2016) examined the consequences of bank fraud on the Nigerian economy's growth. The scope of the study is from 1995 to 2014. The study used secondary data in its analysis. Regression analysis and SPPS application software are being used for data analysis. The study reveals that bank fraud has negative and significant consequences on the growth of the Nigerian economy. Banks' ability to improve economic growth and development in any society is the duty of the extent to which financial activities are carried out with confidence, trust, and least risk. These undoubtedly require a safe and sound banking practice, which many of the banks in Nigeria today have despised to their peril. The study recommends that banks in Nigeria need to improve on their supervision, careful when recruiting employees. Wonderful results alone are not enough, but fear of God and employees' integrity should be considered. The research concluded that the fight for the uncovering, preclusion, and retribution of fraud perpetrators must be tackled to reduce the temptation to commit fraud and increase the chances of detection. While a positive work environment will improve to achieve the former, the latter can be achieved by a sound internal control system

Theoretical Framework

The study adopted the theory of Technology-Enabled Crime as a theoretical framework and the key nature of the theory is that it consists of several categories of criminological theories to help society better understand why crimes co-evolved with computer and telecommunications technologies to become among the most complex and difficult forms of crime to prevent, investigate and control. McQuade (1998) reveals that understanding and maintaining relatively complex crime is initially quite difficult, and there an unending competition between the perpetrators of criminal activities and law enforcement agencies or bodies for technological gains. As the perpetrators of criminal activities do something new and innovative, law enforcement must catch up to avert, control, deter, and prevent new forms of crime.

McQuade (2006) argues that technology-enabled crime theory consists of the following activities. First, crimes committed directly against computers and computer systems. Second, are activities that fall under this category are often referred to as high tech crime, computer crimes, or cybercrimes. The third is the use of technology to commit or facilitate the commission of traditional crimes. Forth is the crimes such as fraud, scams, and harassment can be facilitated using technology which brings unique challenges to old crimes. The theory provides a framework for understanding all forms of criminality and especially those that are evolving with computing and telecommunications technology inventions and innovations. The theory is pertinent for understanding contemporary threats posed by emerging forms of cybercrime, transnational crime, and terrorism networks that defy traditional methods of criminal justice and security measures for preventing and controlling crime (Chamlin & Cochtan, 2007). The theory is also relevant to this study because it provides us insight into the understanding of the new tools and techniques used by cybercriminals; that is, a shift from the simple crime committed using simple tools to the complex crime committed using complex tools. It also helps in understanding the new forms of deviance, social abuse, or crime committed through the innovative use of technology.

Methodology

Data were collected from both primary and secondary source judgmental sampling method was used to select some deposit money banks, out of the 206 questionnaires distributed, 200 questionnaires were utilized, while descriptive statistics, correlation matrix and panel data analysis (Random-effect GLS regression techniques) were utilized as analytical tools in the study with the aid of Statistical Package for Social Sciences (SPSS).

Table 1: The Selected Deposit Money Banks (DMBs) in Kaduna State

S/N	Banks	Respondents	S/N	Banks	Respondents
1	Access Bank Plc	**27**	**5**	GTBank plc	**25**
2	Fidelity Bank plc	**25**	**6**	Keystone Bank	**24**
3	FCMB	**26**	**7**	Stanbic Ibtc	**23**
4	First Bank plc	**30**	**8**	UBA Bank	**26**
	Total				**206**

Source: Field Survey, 2023

Data Presentation and Analysis

During the survey, a total of 206 questionnaires were issued to the bank depositors. The results of the data collected are analyzed below based on each research question, out of the 206 questionnaires distributed, 200 questionnaires were well completed and valid for analysis for this study.

Analysis of response to questionnaire

Questionnaire administration	Frequency	Percentage(100)
Questionnaire Issued	206	100
Questionnaire Return	200	98
Questionnaire not Return	6	2

Source: Field Survey 2023

A total of two hundred and six (206) questionnaires were administered. A total of two hundred (200) (98%) questionnaires were filled and returned while six (2%) questionnaires were not returned by respondents

Data Presentation and Analysis

The results of the data collected are analyzed below based on each research question, out of the 206 questionnaires distributed, 200 questionnaires were well completed and valid for analysis for this study.

Table 2: Frequencies and percentages of sex, position, and year of experience of respondents

Sex Distribution of Respondent	**Frequency**	**Percentage (%)**
Male	115	57
Female	85	43
Total	200	100
Job Position of respondents	**Frequency**	**Percentage (%)**
Top Management	20	10

Senior Management	80	40
Senior Officer	55	28
Junior Officer	45	22
Total	200	100
Years of Experience of respondent	**Frequency**	**Percentage (%)**
1-10	25	13
11-20	45	22
21-30	55	28
31-Above	75	37
Total	200	100

Source: Administered Questionnaire, 2023

Table 2 shows the percentages of sex, position, and year of experience of respondents. Table 2 shows that 57 percent of the total respondents are males, while 43 percent of the total respondents are females. This implies that there are more female respondents than male respondents. Also, Table 2 shows that 10 percent of the total respondents are top management staff of the selected banks, 40 percent of the total respondents are senior management staff, 28 percent of the total respondents are senior officers, while 22 percent of the total respondents are the junior staff. Furthermore, Table 2, shows that 13 percent of the total respondents are between 1-10 years of experience, 22 percent of the total respondents are between 11-20 years of working experience, 28 percent of the total respondents are between 21-30 years of working, 37 percent of the total respondents are between 31-above years of working experience. The results show clearly that a larger percent of the respondents is experienced in the banking industry.

SUMMARY OF FINDINGS

An analysis of the result reveals that:

1. Different types of cyber-crimes have an impact on depositor's accounts and on the Nigerian banking industries.
2. The extent of cyber-crimes has an impact and are significant which can affect the level of depositor's fund safety.
3. The impact of this kind of crime can be felt on the lives, economy and international reputation of a nation.
4. Depositors' fund safety is significantly influenced by the level of cyber-crimes that is carried-out, as it is felt that as more and more cyber-crimes are perpetrated by fraudsters the level of fund safety on the side of the depositors becomes low.
5. Cyber-crime laws/policies and regulations have a positive effect on curbing and mitigating the adverse occurrence of cyber-crimes in Nigeria.

CONCLUSIONS

In conclusion, the research revealed that cybercrimes have a negative impact on online banking transactions and other applications usage by bank customers in Kaduna State. The study also found that there is a high level of banking. cybercrime activities in Kaduna State, banks online protocols against banking cybercrime activities in Kaduna State is adequate, Fight against banking cybercrimes in Kaduna Sate by the related agencies is below expectation, poor Financial literacy and low knowledge of internet operation are the major causes of banking cybercrimes in Kaduna and the awareness creation on banking cybercrimes by all the related agencies are adequate.
There is an insignificant relationship between cyber-crimes and the level of depositor's account. This implies that, the adverse occurrence of cyber-crimes may affect the confidence but will not affect the level of depositor's account,i.e. the more cyber-crimes are carried-out or perpetrated will not affect the level of depositor's trust with their deposits in the bank.

Recommendation

Based on the analysis carried out and the findings made in addition to the review of relevant literature and regression analysis, the following recommendations are necessary;
1. The financial institutions should create an awareness program on cyber-crimes that will help their local depositors' know more about cyber-crimes, how it can be carried out and how they can be affected if measures are not taken.
2. There should be more awareness creation on banking cybercrimes by all the related agencies to reduce the rate of online banking transactions and different types of cybercrimes in Kaduna State
3. The government and the law makers should introduce and implement new policies or laws against cyber-crime perpetrators in the country, in order to further reduce the adverse occurrence of cyber-crimes which leads to loss of depositors' funds.
4. The financial institutions should make sure that there is no any loophole in the internal control system, and make sure all activities are carried out in transparent manner, in order to enhance depositor's trust and confidence.
5. Various banks should revisit the online protocols against banking cybercrime activities in Kaduna state to reduce the rate of online banking transactions.
6.Depositor's should be able to identify authorized and reputable web sites, where they can make their day-to-day transactions, and only supply their bank information's to secured sites, if they must make transactions online, and should report to their local banks if there is any suspect of leak of information.

REFERENCES

Abdulrasheed, S., Babaitu, D., & Yinusa, G. (2012). Fraud and its implications for bank performance in Nigeria, International Journal of Asian Social Science, 2 (4), 35-45.

Anderson, R, C. Barton, R. Böhme. M. J. van Eeten, M. Levi, T. Moore and S. Savage, (2013). "Measuring the Cost of cybercrime" in R. Böhme (ed.), The Economics of Information Security and Privacy (Springer), Chapter 12.

A Summary of the Legislation on Cybercrime in Nigeria, Legislative & Government Relations Unit, Public Affairs Department,Federal Bureau of Investigation (2016). ATM skimming, Retrieved June 8, 2016 available online: https://www.fbi.gov/news/stories/2011/july/atm_071411.

Berney, L. (2008). "For online merchants, fraud prevention can be a balancing act". *Cards & Payments*, 21(2), 22-7.

Biener, C., M. Eling and J. Wirfs, (2015). "Insurability of Cyber Risk: An Empirical Analysis", *The Geneva Papers*, 40.

Böhme, R., S. Laube and M. Riek, (2017). "A Fundamental Approach to Cyber Risk Analysis", *Variance Journal*, Article in Press.

Cebula, J.J. and L.R. Young, (2010). "A taxonomy of Operational Cyber Security Risks", Technical Note CMU/SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University.

Ewepu G, (2016).Nigeria loses N127bn annually to cyber-crime— NSA available at:http://www.vanguardngr.com/2016/04/nigeria-loses-n127bn-annually-cyber-crime nsa/Retrieved Jun. 9, 2016.

Gates, T. and Jacob, K. (2009). Payments Fraud: Perception versus Reality, *Economic Perspectives*, 33(1), 7-15.

Hassan, A. B. Lass F. D. and Makinde J. (2012).Cybercrime in Nigeria: Causes, Effects and the Way Out, ARPN *Journal of Science and Technology*, 2(7), 626 – 631.

Hutchison S. &Davis, W. R.(2003) Computer Crime in Canada, Toronto: Thompson Canada Limited.*Journal of science. 2.*

Idolor, E. J. (2010). Bank Fraud in Nigeria: Underlying Cause, Effects and Possible Remedies: *African Journal of Accounting, Economics, Finance and Banking Research,* 6 (6) pp 62.

Jaishankar K., (2007). Space Transition Theory of Cyber Crimes, Crimes of the Internet, Pearson, ISBN-13:978-0-13-231886-0 pp.283-299.

Lakshmi P. andIshwarya M. (2015).Cyber Crime: Prevention & Detection,"*International Journal of Advanced Research in Computer and Communication Engineering*, 4(3).

Longe, O.B &Chiemeke, S.C. (2007). Beyond Web Intermediaries: Framework for Protecting Web Contents on Clients Systems. Paper Presented at the International Conference of the International Association of Engineers (IAENG) Imperial

Longe, O.B.&Chiemeke, S.C. (2008). Cybercrime and Criminality in Nigeria What roles are internet Access Points in Playing. *European Journal of Social Sciences*, 6 (4).

Maitanmi, O. Ogunlere, S. andAyinde S. (2013).Impact of Cyber Crimes on Nigerian Economy,*The International Journal of Engineering and Science (IJES*, 2(4), 45–51.

MichaelA., Boniface., A. and Olumide, A. (2014).Mitigating Cybercrime and Online Social Networks Threats in Nigeria, *Proceedings of the World Congress on Engineering and Computer Science Adu Michael Kz*, 1 WCECS 2014, 22–24.

Moore, R. (2005). "Cybercrime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.

Moore, Clayton & Anderson (2009).The economics of online crime. *International journal of e-banking and finance,* 55.

McQuade, S. (1998). Towards a theory of technology-enabled crime, unpublished manuscript. George Mason University, Fairfax, Virginia.

Nida T., (2018). Impact of cyber-attacks on financial institutions. *Journal of internet banking and commerce, June 2018.* 23(2). (http://www.icommercecentral.com).

Okeshola F.B. and Adeta A.K, (2013).The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria,*American International Journal of Contemporary Research*, 3(9), 98-114.

Ojo, J. A. (2008). "Effect of Bank Frauds on Banking Operations in Nigeria".*International Journal of Investment and Finance*, 1 (1), p 103.

Okpara, G. C. (2009). "Bank failure and persistent distress in Nigeria: a discriminant Analysis". *Nigerian Journal of Economic and Financial Research.*2(1).

Office of Financial Research, 2017, "Cybersecurity and Financial Stability: Risks and Resilience", OFR Viewpoint, February.

Olasanmi, O. O (2010). Computer Crimes and Counter Measures in the Nigerian Banking Sector. *Journal of Internet Banking & Commerce*, 15(1), 1-10 (http://www.arraydev.com/commerce/jibc/)

Parthiban L. and Raghavan A. R. (2014).The effect of cybercrime on a Bank's finances,*International journal of Current Research and Academic Review*,2(2), ISSN:2347-3215, 173–178, Retrieved Feb. 2014 from www.ijcrar.com

Roger, E.S. (2008). Rogers Communications Inc, 2008 Annual Report

Romanosky, S. (2016). "Examining the costs and causes of cyber incidents", *Journal of Cybersecurity*, 2 (2).

Shandilya, A. (2011). Online Banking: Security Issues for Online Payment Services. www.buzzle.com/articles.

Siddique, M.I. and Rehman, S. (2011). Impact of Electronic Crime in Indian Banking Sector: an overview, *International Journal of Business and Information Technology*, 1(2), September, 159-164.

Soni, R.R. and Soni, N. (2013). An Investigative Study of Banking Cyber Frauds with Special Reference to Private and Public Sector Banks, *Research Journal of Management Sciences*, 2(7), 22 27 July.

Steven M., Robyn M., Anika H., Cameron B., Stefan K., & Eva I., (2013). Comprehensive Study on Cybercrime. *A journal on United Nations Office onDrug and Crime,* (UNODC).

Udegbunam, R. I. (1998). "Bank Failure in Nigeria since Deregulation: Underlying Causes and Implication for Policy". *Benin Journal of Social Sciences*, 6 & 8, (1 & 2).

Vakkari, S.P. (1996). Library and information science: Content and scope. In J. Olaisen, E. Munch-Petersen, & P. Wilson (Eds.), Information science: From development of the discipline to social interaction. Oslo, Norway: Scandinavian University Press.

Wall, D.(2001). Hunting Shooting, and Phishing: New Cybercrime Challenges for Cybercanadians in The 21st Century. The ECCLES Centre for American Studies. http://bl.uk/ecclescentre,2009.

Wilson, P., Kunz, M.(2004). Computer crime and computer fraud. Report to Montegmery County Criminal Justice Coordination Commission, http://www.mongomerycountymd.gov (accessed September 2007).

Willson, R. (2006). Understanding the Offender/Environment Dynamics for Computer Crimes. *Information Technology and People*, 19(2), 170-186.

Wada F. and Odulaja G. O. (2014). "Electronic Banking and Cyber Crime in Nigeria – A Theoretical Policy Perspective on Causation,"*Afr J Comp & ICT*, 4(3), no. Issue 2.