Nwafor M.C., (2018). Impact of Cyber Insecurity in the Development of Online Banking in Nigeria
GO-Uni Journal of Management and Social Sciences 6(1), 14-30
ISSN: 2550-7265

IMPACT OF CYBER INSECURITY IN THE DEVELOPMENT OF ONLINE BANKING IN NIGERIA

Michael Chukwunaekwu Nwafor
Department of Accounting and Finance
Godfrey Okoye University, Enugu
michaelandstephens@yahoo.com

Abstract

This work reviewed the impact of cyber insecurity on development of online banking in Nigeria. Activities that lead to the insecurity of the cyber space known as cyber-crimes were identified as phishing, cyber terrorism, electronic spam mails, cyber stalking and bullying, identity theft and online scam. These activities seriously affect online banking because it is the main target of cyber criminals who aims at siphoning the hard earned money of unwitting individuals. Unemployment and quest for quick riches are the main reasons cyber-crimes are on the increase. Nigerian has been without a law that appropriately address cyber-crime and other related issues until 2015 when a law was put in place. Though online fraudsters have not been prosecuted by this law it is hoped that the presence of the law will serve as a deterrent to people aspiring for a career in cyber-crime which some view as a lucrative venture. Banks, Bank customers, Judiciary, Law enforcement agencies and the government have critical role to play to ensure that activities that cause cyber insecurity in Nigeria are effectively tackled to ensure the onward development of the already existing E-banking platforms in Nigeria.

Keywords: Cyber Insecurity, Cyber Crime, Online Banking, Hacking, Business Cost

Introduction

The growth and expansion of a country's economy is a function of the state of that country's banking sector and as such, the banking sector of a country needs to be prepared to take on the onerous task of an economic driver. Hence the need to ensure the effectiveness and efficiency in performing the banking sector in their task as economic drivers especially in the area of intermediation between the surplus and deficit units of the economy. Due to the critical role the banking sector plays in the development of economy, many technological innovations have been put up to ease the financial intermediation (the flow of money from savings-surplus to savings-deficit).

As a means of getting first-hand behaviour and preferences of clients, the operators of the banking systems have resorted to the deployment of technologies and operations such as Automated Teller Machine networks, Software Development, Call centre operations and Network management and this also helps the industry to quickly and efficiently respond to the needs of the customer in the shortest possible time and also manage cost of running their businesses. These technologies and operations are also called outsourcing functions (Oluwagbeni, Abah& Achimugu, 2011).

Furthermore, the technological innovations being embraced by banks especially those in Nigeria is due to competition going on in the banking sector as is seen in the development of Electronic platforms (E-platforms) or E-banking or Online banking to aid in information and resource control among banks. E-platforms is simply an electronic medium that aids banks in rendering financial services to their numerous

customers with the customers' place, time and distance not posing a problem. The 1980s is believed to be the advent of electronic banking (Wada & Odulaja, 2013). E-banking has been growing at exceptional levels due to technological advancement of this modern world and also growth recorded in the area of Information and Communication Technologies. It is important to note that E-banking is not only found in countries with developed economies but also in those countries with developing and underdeveloped economies because of the numerous business prospects it extends to the banking sector.

E-banking provides clients and customers the opportunity of assessing banking services from the comfort of not just their homes but any other location they wish to carry out their banking activities when the need arises. ATM has been fingered in many quarters as the most effective delivery channel of the E-banking process (Muyiwa, Tunmibi, & John-Dewole, 2013). Studies have shown that the world is home to about 15 million ATM's and projections are being made that the number might grow to about 30 million and more in the next few years. Noteworthy is the fact that banking hours have been extended beyond office hours and national boundaries due to the advent of E-banking technology (Balachandran & Balachandher , 2000).

E-banking broadens client relationships and loyalty to banks which in turn provides competitive advantage to a bank.In spite of all the positive effects of technological advancements on both the customers and banks, it has increased to a significant level the use of technology in criminal activities like cyber crime. It has made the stealing of money from numerous bank account holders of banks very easy thus relegating the hitherto known form of stealing from banks (bank robbery) to the background (Wada, Longe, & Danquah, 2012). Security issues are special concern of banks due to the fact thatbanking is highly dependent on trust from clients. Cyber crime has been a major source of worry to the banking industry because the activities of this scammers, fraudsters and hackers has made the cyber space insecure for genuine business activities of banks.

Therefore, the dangerposed by hackers, technological disasters, breach of confidentiality of clientinformation and chances for fraud generated by the inconspicuousness of the parties to fraudulent electronic transactions have to be properly managed because banking activities must go on. Cyber crime thrives in the online setting for many reasons like the insecure nature of the internet which leaves computers susceptible to misuse by fradulent internet users, numerous computers connected to the internet thus widening the target base of fraudsters and the unregulated nature of the internet which makes it characteristicallyproblematic to regulate the content and data crossing the network, thus hampering efforts aimed at combatingmischievoususe of the internet.

In Nigeria, cyber crime is becoming a highly profitablebusiness through cyber attacks which involve the theft of personal information, fraud, getting into financial systems illegally and online extortion. Interestingly an underground economy has developed through which cyber criminals earn money by trading cyber crime related goods and services.

Objectives of the study

The study seeks to achieve the following:

1. Ascertainimpact of cyber crime on the development of online banking in Nigeria
2. Recommend measures for combating cyber crimes to bank and the Government.

Cyber Crimes

In Nigeria the giant of Africa, crime and corruption which is in the region of about 75% and 71% respectively constitute the most serious obstacle to economic activities and business followed closely by theft and fraud especially internet scam which is also referred to as cyber-crime. Cyber-crime can be defined as any illegal activity carried out on the cyber space with the intent of defrauding another person. It is also the use of the cyber space for criminal activities. Hacking, tapping of phone lines, privacy violations and use of viruses are the developmental trends cyber-crimes has gone through and most recently the use of internet for spying (espionage) and also for perpetuation of terrorism and international crimes. The embracing of E-banking platforms by Nigerian banks though a welcomed development has led to the proliferation of hackers on the cyber space waiting for unsuspecting people to pounce on as they create fake websites through which banking details of people are collected for fraudulent purposes.

Causes of Cybercrimes in Nigeria

The following are some of the identified causes of cybercrime (Hassan, Lass & Makinde, 2012)

a. Unemployment is one of the major causes of Cybercrime in Nigeria it is a well-known fact that over 20 million graduates in the country do not have profitable employment. This has inevitably amplified the rate at which they take part in criminal activities for their existence.
b. Quest for Wealth is another cause of cybercrime in Nigeria. Youths of today are very materialistic; they are not ready to start small therefore they struggle to level up with their rich counterparts by engaging in cybercrimes
c. Lack of strong Cyber Crime Laws also encourages the perpetrators to commit more crime knowing that they can always go uncaught. There is need for our government to come up with stronger laws and be able to enforce such laws so that criminals will not go unpunished.
d. Incompetent security on personal computers. Some personal computers do not have proper or competent security controls; it is prone to criminal activities hence the information on it can be stolen.

Criminal activities in the Cyber Space

This work will try to look at some of the cyber space crime that are of economic importance to the banking sector. The cyber-crimes are listed according to Longe & Chiemeke, (2008) as phishing, cyber terrorism, electronic spam mails, cyber-stalking, fake copy-cat websites, identity theft and false statements.

1. **Phishing:** Phishing is simply an online attempt to take on the identity of, or impersonate a genuine organisation for the sole aim of convincing users to revealprivate information such as financial details, passwords, usernames and email addresses. For instance, a scammer can open a website that has a domain

name that is closely related to the main site of a bank. An unsuspecting user may be directed to this fake website by clicking on the link in a fake spam email furthermore, users may then fall for the confidence trick of the phishing website and may divulge personal details which in turn exposes the user to identity theft or fraud. Rogers (2008) summarises phishing as not only an avenue for stealing peoples personal information and identity but it is also an act of fraud against genuine businesses and financial institutions that are victimized by phishing.Phishing is also a term used to describe any social engineering misconduct aimed at organisations' or individuals'(customers') information systems (IS) in order to collect private information to be used against organisations to extract some benefit for the perpetrator through the anonymity of identity theft or identity deception acts (Roger, 2008). Phishing poses substantial threats to unsuspecting victims and It has become one of the fastest-growing worldwide threats on the Internet which has made the fight against its continous growth a huge priority for electronic mail service as data suggest that some phishing attacks have swayed up to 5% of their recepients to provide sensitive information to fake websites (Loftness, 2004).

2. **Cyber terrorism:** this is intended to cause serious financial loses to the banking sector. It is also a situation where by internet fraudsters use the online setting to launderillegitimate money gotten from other cyber crime activities which is achieved through the use of money mules who are often harmless Internet users who are hired through websites set up for enticing users into applying for work-from-home jobs as a 'financial officer'. They receive funds into their bank account from cyber criminals, withdraw the money in cash and send the money back to the cyber criminal thus making it impossible for the money to be traced (Symantic Corporation, 2009).

3. **Hacking:** This refers to testing and exploring computer systems, highly skilled computer programming or the practice of accessing and altering other people's computers. Hacking may be carried out either with honest aims or with criminal intent. In relation to cyber crime, refers to the practice of illegally accessing, controlling or damaging other people's computer systems. A hacker may adopt either their own technical knowledge or any of the cyber crime tools and techniques like

a. Malicious software (Malware): this simply means any software that is designed to damage or sabotage computer or programming functions. It can come in form of viruses, worms or trojan which are computer codes that automatically infiltrates computer systems, to damage computer performance or to deliver other types of malware (a backdoor permits a computer to be remotely controlled over a network). Malware may install itself on a computer via a self-propagating mechanism, or when a user clicks on a malicious link in an email, opens a malicious file or visits

a website where malware is hosted (Symantic Corporation, 2009).

b. Botnets: A computer affected by malware are referred to as robots or bot. Network of remotely controlled bot computers are known as botnets. The fraudster controlling the botnet is known as the botmaster and the activities of botnets include launching 'distributed denial of service' (DDoS) attacks (a way bywhich botnets flood a computer system with information thus damaging or shutting down the system); hosting malicious websites (such as money laundering, malware or phishing websites) or obscene content (such as child pornography). The botnet is fashioned in such a way as to shield the creator from being known; scanning for, and exploiting, software vulnerabilities in other computers and websites;and sending large numbers of unsolicited emails known as spam are also functions of botnets. This is considered as an important aid to activities that constitute cyber crime (Symantic Corporation, 2009).

4. **Cyber stalking:** This refers to the act utilising the internet, e-mail, or other electronic communications devices to trail another person (Ellison & Akdeniz, 1998). Online harassment and online abuse are other terms that can be used to decribe this phenomenon. A cyber stalker does not physical pose a threat to their victim but harnesses the opportunity provided by anonymity in the cyber space to intimidate their victims without being noticed using platforms such as websites, chat rooms, discussion forums, blogs and e-mails (Ellison & Akdeniz, 1998).

5. **Fake copy cat websites:** Fake 'copy-cat' web sites takes advantage of clients who are unaccustomed to the use of Internet or who do not know the particular web address of the authentic company that they wish to visit. The customer, believing that they are entering credit details in order to purchase goods from the anticipated company, is instead unknowingly entering details into a fraudster's personal database. The impostor 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 carrying out credit card fraud.

6. **Electronic spam mails:** Spam refers to unsolicited emails, or the electronic equivalent of 'junk mail'. Spam is often circulated in enormous amounts by sending out general emails to large lists of email addresses. Spam may be sent through normal email accounts provided by an ISP, free online email services such as Hotmail, hijacked email servers, offshore companies that specialise in sending bulk mail, or the large number of computers connected to a botnet. Spammers can acquire lists of email addresses by: using different pieces of address-harvesting software to locate, steal, decipher and compile email addresses; hacking into the information systems of organisations; creatingfake websites which fool users into entering their email address on the website; or through buying lists of email addresses on the black market. Spam has a variety of uses including: the mass delivery of legitimate

advertising; the mass delivery of scams and phishing schemes; and the delivery of malware and in turn the expansion of botnets. 419 mails or the Nigerian advance fee frauds which in 1996 was estimated to have cost unsuspecting clientele over five billion dollars (Wood, 1995) and in 2017 it has shot up to 127 Billion dollars.

7. **Identity theft and identity fraud:** Through the use of keystroke loggers, spyware, and phishing websites cyber criminals may obtain a wide range of personal details from unsuspecting customers and this is known as identity theft. These stolen details may then be used to commit 'identity fraud' (such as illegally accessing a victim's bank or credit card account, or taking out loans under a victim's name), sold online to other cyber criminals or used to fabricate fake official documents such as passports. Stolen information may also be used to commit further cyber crimeactivities. For example, a cyber criminal may use a stolen identity to opena new Internet account with an ISP from which to commit criminal acts (Symantic Corporation, 2009).

Theoritical framework

Below are some of the theories that tries to address problems especially security issues ravaging the electronic platform.

Space transition theory

This theory provides an explanation on the nature of the behavior of the persons who bring out their conforming and non-conforming behavior in the physical space and cyberspace (Jaishankar, 2008). Space transition involves the movement of persons from one space to another (e.g., from physical space to cyberspace and vice versa). Space transition theory argues that, people behave differently when they move from one space to another. The postulates of the theory are:

1. Persons, with suppressed criminal behavior (in the physical space) have the tendency to commit crime in cyberspace which ordinarily they would not commit in physical space, due to their status and position.

2. Identity Flexibility, dissociative inconspicuousness and lack of restriction factor in the cyberspace provides the offenders the choice to commit cyber crime

3. Illicit behavior of criminals in cyberspace is likely to be introduced to Physical space which, in physical space may be transferred to cyberspace as well.

4. Erraticundertakings of offenders in to the cyberspace and the dynamic spatio-temporal nature of cyberspace provide the chance to escape.

5.Strangers are likely to unite together in cyberspace to commit crime in the physical space.

6. Persons from closed society are more likely to commit crimes in cyberspace than persons from open society.

7. The conflict of Norms and Values of Physical Space with the Norms and Values of cyberspace may lead to cyber crimes.

Routine Activity Theory

This theory states that three conditionsaid the occurrence of crime. Advocates propose that such events must happen at the same time

and in the same space. Existence of a suitable target, lack ofsecurity, and a motivated offender for the crime to occur are the three conditions that facilitate crime. The assessment of the situation determines whether or not a crime takes place (Wada & Odulaja, 2013).

Opportunity Theory

This theory does focus on the on the opportunities emerge as a result of preventive measures to curb the crime rather than those events that contribute to the crime but Proponents of this theory maintain that crimes transverse between location, time, target, direction, and method of committing the crime. Furthermore, they assert that Opportunity to commit a crime is a root cause of crime and that no crime can occur without the physical opportunity and therefore opportunity plays a role in all crimes, not just those involving physical property thereby reducing opportunity of crime (Wada & Odulaja, 2013)**.**

Technology Theory

The reaction of technology to the cyber crimeproblems rests on the use of computer security theories to design and develop solutions thatoffers authentication, verification, non repudiation and validation. These theories andmodels rely on the use of cryptography,steganography, network protocols, and the use ofsoftware engineering process or models to developsystems that offer some form of protection forusers and the information organization.Cybercrime succeeds on the web today for the reason that theinternet did not incorporate in its protocols from thebeginning a machinery that allows a host toselectively refuse messages (Wada & Odulaja, 2013).

Social Theories

This deals with the theories from the socio scientific point of view aimed at protecting internet users against breaches and information misuse. Just as held in the theory of least possible priviledge whereit is stated that new users of internets aremore susceptible to cyber crime when on the cyber space (Bray, 2002). It is better that new users are well trained and enligtened on what they are up against on the cyber space as a way of minimizing threats. There exists a social theory which postulates that values, perceptions and behaviour can be utilised to change user approach about security as ignorance ignorance and incompetence about theconsequences of security policy abuse is a severeproblem among internet users (Wada & Odulaja, 2013). Human morality can serve as an important factor for ensuring that misuse do not occur on the cyber space (Wada & Odulaja, 2013). The use of strong deterrents to convince potential cyber criminals to desist from such acts will also be a vital tool in combating cyber crime (Wada & Odulaja, 2013).

The Peel Theory

This is a theory on community policing which believes that violators or criminals and victims are usually close and used spatial distribution as a basis for capturing criminals and cracking crimes. This theory incorporates the part to be played by the citizens in reacting to partial and completed crime, crime control, and internal order and makes the police in charge of all crime control and law enforcement activities. We cannot conclude that there is any theory in existence from the criminal justice and policing angle that specifically addresses the problem of cyber crime(Wada and Odulaja, 2013)**.**

Impact of Cyber Crimes on the Nigerian Banking Sector

Electronic information system is obviously very important in modern economy bevause when information fails to circulate, whole sectors of the economy ranging from finance, wholesale, retail trade, transportatin, manufacturing to vital public sector suffers. The safeguarding ofcomputer systems and the data they contain has long been recognized as a critical policy. Cyber attacks or breaches of information security appear to be increasing in frequency and few observers are willing to ignore the possibility that future attacks could have much more severe consequences than what is observed to date. Cyber crimes have devastating economic and security consequences which can undermine the integrity of the financial sector as potential customers are discouraged from patronizing the banking industry. Nigeria is the next hub of cyber criminals and accounts for about 8 per cent of the population of cyber criminals in the world. The development of online banking provides enhanced opportunities for perpetrators of cyber crime as monies can be stolen using wire transfer or account takeover.

Criminals may submit fraudulent online applications for bank loans; disrupt e-commerce by engaging in denial of service attacks, and by compromising online banking payment systems.Identity takeovercan also affect online banking, as new accounts can be taken over by identity thieves, thus raising concerns regarding on the safety and soundness of financial institutions in Nigeria. Unless efforts are intensified in arresting and prosecuting cyber criminals, Nigeria will continue being a safe haven for these criminals. As e-banking continues to develop becomes aneven bigger attraction for cyber criminals.Greater access to credit, information abundance, fastness electronic communications, and intensifiedcompetition among financial institutions make it easier than ever for perpetrators to steal identities and falsify information. The existence of cyber crime in the Nigerian banking sector and its effects on the economy require the formulation of appropriate policies to address them.

The reason why cyber crime was on the increase in Nigeria before 2015 is because according to Ewelukwa, (2011) is that technology is moving faster than the law and if that is the case, what the country runs into is a legal vacuum. In Nigeria at the moment, the advance fee fraud and other fraud related offences Act of 2006, which is part of the laws the EFCC is trying to use to check issues relating to cyber crime and electronic fraud is inadequate because the law essentially covers issues relating to internet services and usage but does not cover the whole range of issues relating to cyber Crime and all sorts of electronic crimes that are prevalent. The issue is that, over the years, Nigeria has developed a lot of legislative bills to check some of these crimes. But quite unfortunately, those bills have not been able to see the light of the day, in terms of being finally enacted into law (Ewelukwa, 2011).

The Nigerian popolace must be made to understand that in e-transaction, it is machine that is involved, not man and therefore fraudsters are always on the look out on how to defraud the system.Essentially, trust is the bedrock of every business, if you do not trust someone, you cannot do business with him. In the Nigeria context, due to the fact that we do not have the relevant laws in place that deal on issues relating to cyber crime, people are bound to be a bit concerned. With the prevalent cases of ATM fraud in Nigeria, people are bound to express reservations. It

is important that government agencies re-orientate people about the use of electronic transactions and also explaine to them some of the measures being taken to hold people accountable when some thing goes wrong.

As long as people are sure of thesystem, there will be tremendous increase on the use of e-banking platforms. Interestingly, cyber crime bill was signed into law in 2015 by former President Goodluck Jonathan but it is believed that the judiciary is probably not aware the authorities the law bears that it has not been fully implemented.Bank Verification Number (BVN) a biometric identification system which consists of an 11-digitnumber that acts as a universal ID across all the banks in Nigeria was implemented in 2015 by the Central Bank of Nigeria and it was introduced to link various accounts to the owner thereby ensuring that fraudulent activities are minmised. For fraudsters, opportunities to extort money and carry out other fraudulent activities arose from the implementation of the BVN. It was detected that fake and unauthorised text messages and phone calls were sent to varioususers demanding for personal information such as their account details. In addition, phishing sites were created to acquire such information forunwholesome activities on the bank account (Omodunbi, Odiase, Olaniyan, & Esan , 2016). Hackers target the openness in the security of various bank structures and transfer money from numerous accounts to theirs.

Most cybercriminals transfer small amounts like 5 naira which are sometimes overlooked by the user without questions raised by the users who assumes this was deducted for either SMS or ATM withdrawal charges. Doing this for over a million accounts enriches most fraudsters (Omodunbi, Odiase, Olaniyan, & Esan , 2016). All these illegal activities listed above have made the Nigerian populace to loose faith in the Nigerian banking sector and this has adversely affected the economic development of the nation.on Nigeria. According to the National Security Adviser (NSA), Maj-Gen. Babagana Munguno (rtd), the 2014 Annual report of the Nigeria Deposit Insurance Corporation (NDIC) reveals between 2013 and 2014, fraud on e-payment platform of the Nigerian banking sector increased by 183% published while another report released in 2014 by the Centre for Strategic and International Studies, UK, estimated the annual cost of cybercrime to Nigeria economy at about 0.08% of our GDP, representing about N127 billion (Adesina, 2017).

The situation being created byNigerian cyber criminals is such that international financial institutions now view paper-based Nigerian financial instruments like bank drafts and cheques with scepticism.Also noticed on the international scene is the blacklisting of Nigerian Internet Service Providers (ISPs) and email providers in e-mail blocking blacklist systems across the Internet with some international companies joining in the blocking of entire Internet network segments and traffic that originate from Nigeria. Newer and more sophisticated technologies are emerging that will make it easier to discriminate and isolate Nigerian e-mail traffic (Adesina, 2017).

The Nigerian Cybercrimes Act of 2015

This was first presented to the public as a bill aimed at putting in place as a stronger legal framework to reduce cybercrime. The bill put in place by the Nigerian Government came up after the revision of alreaady existing laws to tackle te menance of fraud in Nigeria. Cybercrime legislation was put forward by

the Government in September 2008 through a bill titled "A Bill for an Act to Provide for the Prohibition of Electronic Fraud in all Electronic Transactions in Nigeria and for other Related Matters". The bill passed second reading in the Nigerian senate in November 2012 and was signed into law in May 2015 by the then President Goodluck Jonathan.This law has properly defined the cyber crime acts as unlawful with punishments attached to any non-compliance to the law. The Act, known as the Cybercrimes (Prohibition, Prevention etc.) Act 2015 creates a legal, monitoring and institutional framework for the prevention, inhibition, uncovering, investigation and prosecution of cybercrimes and for other related matters. Principally, the Act engenders a policy for cyber security and also ensures the protection of computer systems and networks, electroniccommunications, data and computer programs, intellectual property, privacy rights as well as preservation and protection of the critical national information.

The Cybercrimes Act 2015 is the first legislation in Nigeria that specifically addresses cybercrimes and cyber security. The Act, which was signed into law on May 15, 2015 specifies that, any crime or injury on critical national information infrastructure, sales of preregistered SIM cards, unlawful access to computer systems, Cyber-Terrorism, among others, would be punished. The Act recommends severe penalties for offenders and perpetrators of cybercrime. The Cybercrimes Act is made up of 59 Sections, 8 Parts; and 2 Schedules. 1st Schedule lists the Cybercrime Advisory Council; 2ndSchedule lists businesses to be levied for the purpose of the Cybersecurity Fund under S.44(2)(a): GSM service providers and all telecom companies; Internet service providers; banks and other financial institutions; Insurance companies; and Nigerian Stock Exchange. Some higlights of the act are as ststed below by Adesina(2017):

a. It empowered the president to label certain computer systems, networks and information infrastructure essential to the national security of Nigeria or the economic and social well-being of its citizens as Critical National Information Infrastructure (CNII),and to implement procedures, guidelines, and conductaudits in furtherance of that.Transport,communication, banking are examples of systems that can be labelled CNII.
b. Among other punishments put forward for other cyber crime, the act prescribes death penalty for any crime against Critical National Information Infrastructure
c. If an individual is proven guilty of hacking (unlawfully accessing a computer system) or using electronic messages to comit internet fraud, that individual is liable Five years imprisonment with a fine of ₦10 million.
d. It prescribes punishment for identity theft ranging from 3 years imprisonment or a fine not less than ₦7million or both
e. It prescribes the punishment for procuring, distribution and possession of child pornography as 10 years imprisonment or ₦20 million fine or both depending on the magnitude of the crime committed
f. Itobligates service providers to keep all traffic data and subscriber information with dueregard to the individual's constitutional right to

privacy, and to take appropriate measures to safeguard theprivacy of the data retained, processed or retrieved

g. It prescribed punishment ranging from imprisonment for one to ten years or fine of ₦2.25 million for cyber stalking and cyber bullying.

Empirical Framework

Tunmibi and Falayi (2013) carried out a study that seek to access Information technology security and e-banking in the Nigeria banking sector. They carried out their research using questionnaire administered to a total of forty customers drawn from nine different banks in Nigeria using accidental sampling method.The researchers acknowledged Information technology as the life wire of banks in the financial sector as it promotes and facilitates the performance of banks in various countries. The researchers noted that with respect to IT security in Nigeria, there is a disparity in the level of trust that customers have in their banks as most of the customers they sampled said that network is unreliable and there is an occasional experience of cash deduction without cash withdrawal when using ATM. They concluded by stating that IT security is a major challenge to e-banking in Nigeria and that the Nigerian banking sector is not stable enough for e-banking.

Adesina(2017) in her study titled Cybercrime and Poverty in Nigeria stated that cyber crime is on the increase in Nigeria due to the fact that the young and the old now have access to the world from their homes and offices because of the high level of internet or web-enabled phones and other devices like iPods, and Blackberry in ciculation that have made internet access easier and faster. The author brought to the front burner a new type of cyber crime in Nigeria known as "Yahoo Yahoo" or "Yahoo Plus" which according to the study is a source of major concern to the country. The researcher further posits that Nigeria's rising cybercrime profile may not come as a surprisebecause of the high level of poverty and high unemployment rate in the country. The work recomnended that the government must put practical policies and programmes on poverty reduction and eradication in place and these policies and programmes needs to be astutely backed by actions so as to reduce cyber crime in the country.

Wada and Odulaja (2013) carried out a theoretical study on the policy perspective on Causation of cyber crimes in the Nigerian banking sector. They posited that information communication technology (ICT) revolution has had impacts in almost every area of humanendeavor ranging from business, industry, government to not-for-profit organizations. They furthered stated that ICT has simplified businessprocesses such as sorting, summarizing, coding, editing, customized and generic report generation in a realtime processing mode. Furthermore, they stated that ICT has brought unpremeditated consequences such as criminal activities, spamming, credit card frauds, ATM frauds, phishing, identity theft and other related cyber crimes which they say are adversely affecting the Nigerian Banking Sector. The study also examined the existing policy framework and assessed the success of the institutional countermeasures in combating cyber crime in the banking industry using social theories to explain causation of cyber crimes with a view of guiding policy makers on behavioural issues that should be considered when formulating policies to address cyber criminal activities in Nigeria.

Okoro and Kigho, (2013) carried out a study on the problems and prospects of E-transaction in Nigeria. To achieve this they distributed samples of 350 copies of questionnaire were distributed to users of online banking platforms in Nigeria. They formulated two hypotheses for their study and chi-square statistical tool was adopted in testing the hypotheses. The results obtained by them revealed that there is a significant relationship between e-transaction in promoting economic growth in Nigeria but this has not been moving in the right direction as it is still at its infant stage and the attitude of government, corporate bodies and individuals pose a problem to e-transaction as they are enslaved in fears resulting from insecurity, technical problems, anonymity, cultural problems and so on.

Omondubi et al. (2016) examined the issue of Cybercrimes in Nigeria with particular attention on its analysis, detection and prevention. Their area of study was the various tertairy institutions located in Ekiti state Nigeria. They distributed about 600 copies of the questionnaire to students in the tertiary institutions in the state. On analysis of the questionnaire, it was discovered by the researchers that possession of mobile phones, tablets and laptops by students is the major cause of cyber crimes in the state. They also discovered that most of the respondents have committed phishing which they referred to as a harmless cyber crime.

Ezeoha(2006) carried out a study on regulating internet banking in Nigeria. He maintains that for internet banking to assume a developmental dimension in Nigeria and for the country to be fully integrated in the global financial environment, the prevalent level of frauds in Nigeria (and among Nigerians) must first be addressed. He further suggests that the ways to address fraud in Nigeria are to get the relevant local laws in place and in consonance with international laws and conventions; get the citizens well educated on the complexities of internet usage and frauds, as well as the regulatory implications of wrong or fraudulent uses of the Internet; ensure that all the major background problems such as poverty, corruption and bad governance are addressed and; ensure adequate interface and collaborations between Nigerian local law enforcement agents and the various international agencies that are presenting pursuing the course for safe Internet community.

Aribake (2015) carried out the a theoretical and practical study on the impact of ICT tools for combating cyber crime in Nigeria in other words, study wanted to consider cybercrime and its impact in an online banking in Nigeria. The researcher stated that adoption of ICT in banks really help them to enhance customer services, assisted precise records, guarantee suitable business hour, improve quicker services. The study further reveals that there has been advancement in the image of thebanks which hints to a broader, quicker and more effectual market. Also the fact that ICT tools enable work to be easier and more stimulating was also noted by the researcher. The researcher subjected data gotten from the research instruments used to descriptive analysis and regularity tallies in ways to describe the actions of Nigeria cyber criminals based on online banking and to know the way to use ICT tools in prevent these crimes.

Olusola, Ogunlere, Semiu and Yinka (2013) carried out a research on impact of cyber crimes on Nigerian economy using quetionnaires distributed to about 60 respondents drawn from the bursary department, computer department, students

and some lecturers from Babcock university. The researchers quantitatively analysed the responses gotten using some statistical techniques. The results of the analysis according to the researchers show that cracking, software piracy, and pornography among others are prevalent crimes in Nigeria and that the impacts of these crimes on Nigerian economy cannot be over emphasized. Recommendations were put forward by the researchers on how these crimes can be minimized if not totally eradicated like the creation of a National Computer Crime Resource Centre that will comprise of experts and professionals tocreate rules, regulations and standards of authentication of each citizen's records and the staff of establishments and recognized organization, firms, industries forensics personnel and law enforcement agencies so that a data base will be developed from which people can confirm the identities of people they are dealing with on the internet.

Jegede and Olowookere(2014) carried out a study which examined the opportunities and the negative impacts associated with the use of internet technology in this period of E-Business. The researchers revealed that many Nigerian youths engage in online scam as a means of survival in Nigeria. Futhermore, the researchers stated that the platform provided by the internet has to a great level promoted e-commerce and at the same time created a new form of socio-economic insecurity that is greatly unparalleled in the world history. The researchers further posited that the enormousness of exposure and concurrently the monetary loss often attendant to use of wireless transaction cross culturally stimulates fear, skepticism and disenchantments among internet users in the cyber environment.The researchers put up some recommendations to help minimise the trend observed above which includes the creation of a special inbuilt security mechanism that can be attached to the internet technology whkich serves in providing censorship for online monetary related interactions which will help check fraud in the cyber space.

Chigozie-Okwum, Ugboaja, Micheal, & Osuo-Genseleke (2017) carried out a study on Proliferation of Cyber Insecurity in Nigeria. Their study used a survey methodology which entailed the use of interview sessions for data collection. 50 respondents were purposively sampled and the data so collected were analysed by them using the 5 WHYs method of root causes analysis. The researchers identified poor promotion of cyber security professionals' recruitment, training, and upgrade in technical knowledge and development in Nigeria; lack of feasibility and workability analysis of the resultant effects of certain policies on the overall economic sector of the nation, sabotage by monitoring and regulation agencies which render the energy sector unfunctional; and sabotage by the elite class for personal gains and poor funding of the security agencies as the root causes of the increase in cyber insecurity in Nigeria. The reserchers highlighted periodicprevention approaches to these root causes, such as the establishment of world class cyber security training institutions to train digital forensics investigators, and ethical hackers on global best practice and ways of combating the activities of cyber criminals among other strategies.

Ebem, Onyeagba, and Ugwuonah (2017) carried out a study on internet banking focusing on solutions to identity theft. They tried to show the association between lack of proper information dissemination techniques, computer literacy and high rates of identity theft or financial crimes in Nigeria. They

used questionnaire which were distributed to randomly selected internet-banking users and also interviews were conducted on the selected internet users. From their findings, they reached the compromise that lack of proper knowledge and means or forms of identifying cyber crime related emails, texts and phone calls are responsible for the high rate of identity theft in Nigeria because. Also they stated that cyber criminals are exploring other forms of social engineering because according to the researchers, the cyber criminals know that banks will never ask for financial information through emails.

The above numerous works by various scholars shows how much the issue of cyber insecurity threatens financial inclusion and deepening in Nigeria. Ironically, the insecurity of the cyber space is the very reason banks protect financial information of their customers. Thus, the treat coming from hackers serves as a major check to the financial looseness of the banking industry in Nigeria – although at a price. The world is progresively digitizing everything, gone are the days companies invest more in marketing. Proactive bank managers invest more in cyber security – the security of their financial space on the web. The cost of letting a financial vulnerablity into the hands of a hacker for a minute could cause a major financial loss that would shake the asset base of the bank.

Recommended Remedy to Online Banking Frauds in Nigeria

Development of online banking in Nigeria will suffer a major set back if all the crimes rendering the cyber space insecure for genuine business are not tackled headlong.

The government should as a matter of urgency ensure that cyber criminals are prosecuted when caught according to the provisions of the cyber crime law 2015. Government should also intensify efforts on the training and re-training of law enforcement agents so that they cannot be out smarted by the cyber crimininals who of course are very smart in their dealings. Staff of Government agencies involved in the tracking of cyber criminals should make sure that they always update themselves on the recent developments in the area of crime in the cyber space.

In the case of identity theft, it is note worthy to mention that it is not possible without the 'cooperation' of the target as it is genuine account holders that part with confidential financial information due to either carelessness, negligence or ignorance except when their systems are infected by malwares desribed above. So it is important for bank clients that make use of online banking platforms to always be on the look out to avoid divulging sensitive information to fraudsters (making their job easy by bringing the information they need to perpertuate crime to their door step).

Use of antivirus softwares that can block malwares from functioning properly in the systems of online banking users. The banks have a larger role to play in this perspective. Available statistics reveal that over 70% of identity theft targets are people within the agebracket of 40-70 years who have very limited or no knowledge of ICT. This population comprises of the market women, artisans, civil servants (both retired and active), commercial drivers who had very little formal education and can scarcely read or write.

The advent of cashless policy in the Nigerian banking sector have forced people who were withdrawing money before now over the counter to now resort to the use of ICT and

its tool as a means of carrying out business transactions. Due to their scarce knowledge of ICT, these people are vulnerable to being attacked by cyber criminals. Grassroot awareness campaign should be carried out in village town hall meetings, churches, Mosques, Motor parks and other places where unschooled and old people are in large concentration and the sensitization should ne conducted by bank officials in the local dialects of the target population.Radio jingles, television adverts and periodic reminders through emails and text messages can also help the younger generations in fighting identity theft.

Banks on their own part shouldmake sure that their customer service phone numbers are toll free as this will ensure easier access to the banks from their customers.Nigerian tertiary institutions produce about six hundred thousand graduates every year out of which about 50% are skilful in the use of ICT and the internet(Samuel, Bassey, & Samuel, 2012). The Nigerian employment market can scarcely engage only about 20% of these graduates and the necessary economic and social infrastructures which are essential to successful start-ups of Small and Medium scale Enterprises (SMEs) are practically non-existent so some of this mass of unemployed youths resort to cybercrime as a means of survival.

Fixing of the social and economic infrastructures by the Nigerian Federal Government should aid in reducing cyber crime in the country as a failure in doing so will attract more highly skilled cybercriminals to the Nigerian Cyber space thus causing more loses for thefinancial sector (Heydati, 2014).

Conclusion

The Nigerian banking sector must not relent in its resolve to join other banking sectors of the world in the adoption of techmology to aid banking activities because of all the activities listed in the work which leads to cyber insecurity. Nigerian banks must put in place measures to ensure that they and their customers do not fall prey to cyber crime capable of putting them out of business. They must ensure that they employ the use of strong firewalls to prevent malware attacks to their systems. Bank staff must be trained on the steps to take ifa malware attack is noticed before the arrival of an engineer. On the part of bank customers, they should understand that care should be taken when releasing financial information online as any mistake can lead to loses to the customer. Government should make sure that on their part, cyber criminals when apprehended are made to face the full weight of the law according to the provisions of the cyber crime laws 2015.

References

Adesina, S. O. (2017). Cybercrime and Poverty in Nigeria. *Canadian Social Science*, 19-29.

Aribake, F. O. (2015). Impact of ICT tools for Combating Cyber Crime in Nigeria Online Banking: A conceptual Review. *International Journal of Trade, Economics and Finance*, 272-277.

Balachandran, & Balachandher , K. G. (2000). E-Banking Development in Malaysia: Prospects and Problems. *Journal of International Business Management*.

Bray, T. J. (2002). Security actions during reduction in workforce efforts: what

to do when downsizing. *Information System Security*, 11-15.

Chigozie-Okwum, C., Ugboaja, S., Micheal, D., & Osuo-Genseleke, M. (2017). Proliferation of Cyber Insecurity in Nigeria: A Root Cause Analysis. *International Journal of Science and Technology (STECH) Bahir Dar-Ethiopia*, 53-60.

Ebem, D. U., Onyeagba, C. J., & Ugwuonah, G. E. (2017). Internet Banking: Identity Theft and Solutions- The Nigerian Perspective. *Journal of Internet Banking and Commerce*, 12-23.

Ellison, L., & Akdeniz, Y. (1998). Cyber stalking: the Regulation of Harassment on the internet. *Criminal Law Review*, 29-48.

Ezeoha, E. A. (2006). Regulating Internet Banking In Nigeria : Some Success Prescriptions– Part 2. *Journal of Internet Banking and Commerce*.

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

Heydati, A. (2014). An analysis of identity theft: Motives, Related frauds, Techniques and Prevention. *Journal of law and conflict resolution*.

Jaishankar , K. (2007). Establishing a Theory of Cyber Crimes. *International Journal of Cyber Criminology*, 2-9.

Jegede, A. E., & Olowookere, I. E. (2014). Cyber Risks and Fraud in the Nigeria's Business Environment: A Postmortem of Youth Crime. *Journal of Social and Development Sciences*, 258-265.

Loftness, S. (2004). *Responding to phishing attacks.* Glenbrook partners.

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*.

Muyiwa, O., Tunmibi, S., & John-Dewole , A. T. (2013). Impact of cashless economy in Nigeria. *Greener Journal of Internet, Information and Communication Systems*, 40-43.

Okoro, E. G., & Kigho, P. E. (2013). The problems and prospects of E-transaction (The Nigerian Perspective). *Journal of Research in International Business and Management*, 10-16.

Olusola, M., Ogunlere, S., Semiu, A., & Yinka, A. (2013). Impact of Cyber Crimes on Nigerian Economy. *The International Journal Of Engineering And Science*, 45-51.

Oluwagbeni, O., Abah, J., & Achimugu , P. (2011). The impact of information technology in Nigeria's banking industries. *Journal of computer science and engineering*, 11-20.

Omodunbi, B. A., Odiase, P. A., Olaniyan, O. M., & Esan , A. O. (2016). Cybercrimes in Nigeria: Analysis, Detection and Prevention. *FUOYE Journal of Engineering and Technology*.

Rogers, E. S. (2008). *2008 Annual report.* Rogers Communication Inc.

Samuel, A., Bassey, O., & Samuel, I. (2012). Graduate Turnout and Graduate Employment in Nigeria. *International Journal of Humanities and Social Sciences*, 254-258.

Symantic Corporation. (2009). *Report on the Underground Economy july 07-june 08.* Symantic Corporation.

Tunmibi, S., & Falayi , E. (2013). IT Security and E-Banking in Nigeria . *Greener Journal of Internet, Information & Communication System* , 61-65.

Wada, F., & Odulaja, G. O. (2013). Electronic Banking and Cyber Crime

In Nigeria - A Theoretical Policy Perspective on Causation. *Afr J Comp & ICT*, 69-82.

Wada, F., Longe, O., & Danquah, P. (2012). Action speaks louder than words – understanding cyber criminal behavior using criminological theories. *Journal of internet banking and commerce*.

Wood, C. C. (1995). Is security awareness raising methods. *Computer Fraud Security Bulletin*, 13-15.