International Journal of Social Sciences and Humanities Reviews Vol.10 No.1, January 2020; p.66 – 76, (ISSN: 2276-8645)

THE ROLE OF INFORMATION TECHNOLOGY IN CURBING THE CHALLENGES OF INTERNET AND CYBERCRIME IN NIGERIA

NWANKWO ECHEZONA PRISCA
Nnamdi Azikiwe University, Awka
E-mail: echeenwaprisca@gmail.com

Abstract
Information Technology has become a dynamic and extremely powerful means of collecting, processing, storing, presenting and sharing information in the developing countries. The processed information is usually presented on digital devices, and also to a large extent presented on public infrastructures such as the internet and the World Wide Web. Information Technologies have become widespread and have penetrated deeply into societies in developing countries. The proliferation of Information Technology (IT) has resulted in the change of different aspects of human life, bringing convenience and simplicity to our lives. The contribution of the internet to the development of Nigeria has had a positive impact on various sectors of the country. However, it has come with its own share of problems, which have become one of the major challenges of insecurity in Nigeria. Though it makes life so speedy and fast, but hurled under the eclipse of threat from the deadliest type of criminality termed as 'Cybercrime'. Cyber-crime consists of a variety of criminal acts perpetrated through the Internet, and includes e-mail scams, child pornography, hacking, theft of data, spamming, Automated Teller Machine spoofing, piracy, phishing, identity theft, extortion and a wide array of other nefarious activities. Amidst of these threats of insecurity with cybercrime, Information Technology still has a lot of roles to play to curb these challenges in Nigeria Development. The study sets to find out the roles of information technology in curbing internet and cybercrime.

Keywords: information technology, internet, cybercrime

Introduction

Today computer networks are more accurately referred to as information systems. The largest information system in the world is the Internet, although there are many regions and parts to this giant network. The Internet is seen as part of the globalization process that is supposedly sweeping away old realities and certainties, creating new opportunities and challenges associated with living in a 'shrinking' world. We are now said to be in the midst of a 'new industrial revolution', one that will lead us into a new kind of society, an 'information age' (Webster, 2003).These social transformations wrought by Internet technologies has made the future appear insecure and unpredictable, yielding public and political overreaction. Such 'moral panics', fueled by the media, lead to an excessive and unjustified belief that particular individuals, groups or events present an urgent threat to society (Critcher, 2003). Internet-related instances of such panics include those over the effects of pornography in the mid-1990s, and more recently over threats to child safety from pedophiles (Littlewood, 2003). The emergence of the World Wide Web, along with a myriad of software applications, online content, and the beginning of broadband internet connections, computer crime has evolved into computer-related crime and then what we refer today as cybercrime.

Africa has seen a phenomenal growth in Internet connectivity in recent years. With the increasing availability of broadband connections and the decrease in subscription fees, the number of new online users in Africa is outpacing the rest of the world. According to Internet World Stats, Internet use in Africa had reached 2.3 per cent of the total worldwide use by December 2007.4 Africa's internet usage from 2000 to 2007 increased by 423.9 per cent compared to 180.3 per cent for the rest of the world. This high number of users in Africa has made the Internet a popular means of communication as well as opening new opportunities for online enterprise, and likewise, a similar increase in cyber-criminal activities requiring an increased effort across the region to strengthen the information infrastructure, educate users in security awareness, and develop

cyber-crime regulations. The potential for internet abuse is even greater in and for Africa. Due to the lack of security awareness programs or specialized training for the law enforcement agencies, many online users are becoming victims of cyber-crime attacks and the incidence of successful attacks is increasing with impunity.

According toVladimir (2005) Internet already turn to become a worldwide network according which brings together millions of computer situated in various countries and also exposed broad chances in obtaining and interchange data which is now been used by so many for illegal acts, Nigeria's reputation has suffered greatly due to the increase of cybercrime in the country. In the years before full penetration of the internet and mobile technologies, Nigeria had already gained the reputation of one of the most corrupt countries. However, as internet penetration and technologies gained ground, the situation has grown worse as financial crimes and other forms of crime have escalated with the use of the internet and new mobile technologies. This has caused Nigeria to lose a lot of foreign exchange from business and opportunities from investors. A stigma has been created for Nigeria and almost every Nigerian outside the country is observed suspiciously as a perpetrator of crimes. Nigeria as a whole has been stigmatized as a nation whose citizens are mostly untrustworthy. This has brought about serious embarrassment when Nigerians have to travel to foreign countries; extra searching at airport as well as denial of opportunities because of high rate of cybercrime and other related offences common to Nigerians (Olanrewaju and Adebiyi, 2014).
In the years 2007 internet crime report itemized Nigeria name as third in terms of online crime action and the occurrence of cybercrime amid the sufficiently number of young Nigeria (Sesan, 2010). Cyber-crime involves 'action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data (Council of Europe (COE), 2001). Cybercrime can simply be explained as crimes carried out with the aid of a computer system against an individual, organization or a nation (Hassan, Lass and Makinde, 2012). Others sought to classify cyber-crime into computer-related and content-based species (Walden, 2003; Lewis, 2004) or between 'true cyber-crime'– dishonest or malicious acts that would not exist outside online environment and 'e-enabled crime' – criminal acts already known to the world but now promoted through the internet (Burden, Palmer, and Lyde, 2003).

Schell (2004) defined cybercrime as a crime related to technology, computers and the internet and it concerns governments, industries and citizens worldwide where cybercrime takes the form of either piracy, phreaking (obtaining free telephone calls), cyberstalking, cyberterrorism and cyber pornography. Milhorn, (2007) on the other hand, simply defines cybercrime as any activity that uses the internet to commit a crime. Cyber-crime consists of a variety of criminal acts perpetrated through the Internet, and includes e-mail scams, child pornography, hacking, theft of data, identity theft, extortion and a wide array of other nefarious activities. Other IT–related crimes include the counterfeit cashier's cheque scheme, which relies on the issuance of fraudulent cheques, and targets individuals that use Internet advertisements to sell merchandise. Another is the advance fee fraud, also known as the "419 scam", after the section of the Nigerian Criminal Code dealing with the crime of obtaining property by false presences. The 419 scam combines impersonation fraud with a variation of an advance fee scheme, and relies on letters, emails, or faxes to potential victims from individuals representing themselves as government officials, offering the recipient the "opportunity" to share in a percentage of millions of dollars, while soliciting for help in placing large sums of money in overseas bank accounts. Cybercrimes are offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, or deny someone of what belongs to him/her, using modern telecommunication networks such as Internet and mobile phones. Such crimes may threaten a nation's security and financial stability.

Mbaskei (2008) in his publication on "Cybercrimes: Effect on Youth Development" noted that secret agents of the UPS (United Parcel Service) smashed a record scam with a face value of $2.1billion (about N252 billion) in Lagos. The interception was done within three months. Some of the instruments uncovered by the

UPS were documents like Wal – Mart Money orders, Bank of America cheques, U.S postal service cheques and American Express traveler's cheques. This record scam is made possible as a result of the large number of young people who now see Cybercrimes or internet fraud as a source of livelihood. Therefore, these reports are consistent with recent submission in Ekoa and Mungwe (2018), that Nigeria cybercrime has evolved from silly spray-and-spray email spam campaigns to refined con games that target large business organizations. According to the report, it is noteworthy that over 8,400 malwares sample was derived from Nigeria's scam emails from July 2014 to June 2016.

The problem of cybercrime is a global one whose extent, magnitude and impact reverberate throughout various walks of life, leaving hitherto unimaginable damage in its wake. Popularly referred to as the "yahoo yahoo syndrome" in Nigeria, these fraudulent activities are carried on by a recalcitrant few, but the impact is far reaching due to the world-wide reach of the Internet. Cybercrime is not only an embarrassment; it also has negative implications for the positive deployment of IT for socio-economic growth and development. Cyber-crime has indeed reached epidemic proportions. In a relatively recent survey, more than 90 percent of the respondent corporations and government agencies reported computer security breaches at one time or the other. It is commonplace for disgruntled employees and hackers to commit many cyber-crimes while others are committed by crooks using the Web to perpetrate auction fraud, identity theft and other scams. Financial institutions invariably get hit hard as identity thefts reportedly cost them $2.4 billion in losses and expenses in 2000 alone (Hansen, 2002).

All stages of computer operations are susceptible to criminal activity, either as the target of fraud, the instrument of fraud, or both. Input operations, data processing, output operations and communications have all been utilized for illicit purposes. The more common types of computer fraud include, fraud by computer manipulation where intangible assets that are represented in data format such as money on- deposit or hours of work, are the most common targets of computer related fraud. Modern business is replacing cash with deposits transacted on computer systems, creating an enamor potential for computer fraud. The organized criminal community has targeted credit card information, as well as personal and financial information about clients. The sale of this information to counterfeiters of credit cards and travel documents has proven to be extremely lucrative (Siegel, Saukko & Knupfer, 2000).

Cyber-crime is motivated by fraud, typified by the bogus emails sent by 'phishers' that aim to steal personal information. The tools driving their attacks and fueling the black market are crime ware - bots, Trojan horses, and spyware (Lininger and Dean, 2005). Phishing threats on the other hand, are inform of hacking of vital information especially hacking of credit card information or account information. In attempting exposure reduction to common security threats, the top managers must carry out risk assessment of both internal and external threats to know and identify where risks may come from (Akinsuyi, 2009). Spyware has occupied the center stage of late, it is but one of the tools behind today's rash of cyber-crime. Deceptive Trojan horses, multi-purpose bots, and spyware programs form the crime ware arsenal of today's hackers and are regularly bought and traded on the illicit market. The price tag of crime ware is often based on their ability to steal sensitive data such as bank and credit cards while remaining undetected by the victim. Whatever the case, it is obvious that cyber-crime may be targeted against natural persons, property, or institutions.

Viruses, Trojans and Worms all fall into a similar category as they are software designed to infect computers or install themselves onto a computer without the users' permission, however they each operate very differently. A typical virus does two things, first, it copies itself into previously uninfected programs and secondly, it executes other instructions that virus creator has included in it. Some viruses do not have any harmful instructions at all, instead they cause damage by replicating and taking up disk space (Adomi, 2008).

Causes of Cybercrimes in Nigeria

The following are some of the identified causes of cyber-crime (Hassan, 2012)

a. Unemployment is one of the major causes of Cybercrime in Nigeria. The rate of unemployment in Nigeria is alarming and growing by the day. Companies are folding up and financial institutions are going bankrupt. It is a known fact that over 20 million graduates in the country do not have gainful employment. This has

automatically increased the rate at which they take part in criminal activities for their survival. The federal government has proposed a mass sack of government workers. Companies are also embarking on mass sacks of staff. Financial institutions have put unreasonable age barriers on who is eligible to apply for jobs and embarked on mass lay-offs of staff based on ad-hoc decisions.

b. Poverty Rate: On the global scale, Nigeria is regarded as a third world country. The poverty rate is ever increasing. The rich are getting richer and the poor are getting poorer. Insufficient basic amenities and an epileptic power supply have grounded small scale industries.

c. Quest for Wealth is another cause of cybercrime in Nigeria. Youths of nowadays are very greedy, they are not ready to start small hence they strive 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. Corruption: Nigeria was ranked third among the most corrupt countries in the world. Until 1999, corruption was seen as a way of life in Nigeria.

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.

Poonia, Bhardwaj and Dangayach (2011) listed types of Cyber Crime such as:

1. Communications in Furtherance of Criminal Conspiracies: Just as legitimate organizations use the information networks for record keeping and communication, so too are the activities of criminal organizations enhanced by the advent of information technology. There is evidence of information systems being used in drug trafficking, gambling, money laundering and weapons trade just to name a few.
2. Telecommunications Piracy: Digital technology permits perfect reproduction and easy dissemination of print, graphics, sound, and multimedia combinations. This has produced the temptation to reproduce copyrighted material either for personal use or for sale at a lower price.
3. Electronic Money Laundering: For some time now electronic funds transfers have assisted in concealing and moving the proceeds of crime. Emerging technologies make it easier to hide the origin and destination of funds transfer. Thus money laundering comes to the living room.
4. Cyber Terrorism: A cyber terrorist can be described as someone who launches attack on government or organization in order to distort and or access stored information stored on the computer and their networks. It means that any act intended to instill fear by accessing and distorting any useful information in organizations or Government bodies using Computer and Internet is generally referred to as Cyber Terrorism. Another form of cyber terrorism is cyber extortion is a form of cyber terrorism in which a website, e-mail server, computer systems is put under attacks by hackers for denial of services, demanding for ransom in return. Cyber extortionists are increasingly attacking corporate websites and networks, crippling their ability to operate and demanding payments to restore their service.
5. Botnets: Botnets are networks of hijacked personal computers that perform remotely commanded tasks without the knowledge of their owners. A computer is turned into a bot after being infected with specific type of malware which allows remote control. Botnets are used for a wide variety of crimes and attacks: distributing spam, extending malware infections to more computers, contributing to pay-per-click fraud, or identity theft. One of the most worrying uses of botnets is to perform distributed denial of service (DDoS) attacks. Researchers and cybersecurity companies have warned that botnets are becoming the biggest Internet security threat, as they are increasing the effects of viruses and other malicious programs, raising information theft, and boosting denial of service attacks.
6. Fraud - Identity Theft: Fraud is a criminal activity in which someone pretends to be somebody and retrieve vital information about someone. For instance, making a false bank webpage to retrieve information of account of someone. The concept is simple; someone gains access to your personal information and uses it for his own benefit. This could range from a black-hat hacker stealing online banking account login and password to getting access to ATM and using such people can make themselves a lot of money with personal information. In Nigeria people design web links forms

requesting users to fill in their basic information including, unique details like pin numbers and use that to commit crimes.

7. Denial of service (DoS) attacks: These attacks involve flooding a computer or website with information, preventing them to function properly. These attacks are aimed to exhaust the resources available to a network, application or service, in order to prevent users from accessing them. They are more frequently aimed at businesses, rather than individuals. Distributed denial-of-service (DDoS) attacks are those attacks in which multiple compromised computers attack a single target. A DoS attack does not usually result in the theft of information or other security loss, but it can cause financial or time loss to the affected organization or individual, because of its effects (particular network services becoming unavailable, websites ceasing operation, targeted email accounts prevented from receiving legitimate emails, etc.)
8. Illegal Interception of Information: Developments in telecommunications as well as data transfer over the net have resulted in greater speed and capacity but also greater vulnerability. It is now easier than ever before for unauthorized people to gain access to sensitive information.
9. Malware: Malware refers to viruses, Trojan horses, adware, spyware, worms and other software that gets onto your computer without you being aware it's there. In some cases, a piece of malware will pretend to be a legitimate piece of software. When such software is downloaded, it infects the computer system and destroys valuable information. A virus can replicate itself and spread to other devices, without the user being aware. Although some viruses are latent, most of them are intended to interfere with data or affect the performance of devices (reformatting the hard disk, using up computer memory, etc). A trojan horse is a type of malware that is often disguised as legitimate software. Trojans can be employed by cyber-thieves and hackers trying to gain access to users' systems. Users are typically tricked by some form of social engineering into loading and executing Trojans on their systems. Once activated, Trojans can enable cyber-criminals to spy on users, steal sensitive data, and gain backdoor access to users' system. The Trojan horse is also a technique for creating an automated form of computer abuse called the salami attack, which works on financial data. This technique causes small amounts of assets to be removed from a larger pool. The stolen assets are removed one slice at a time. Adware collects marketing data and other information without the user's knowledge, or redirects search requests to certain advertising websites. Spyware monitors users, gathers information about them and transmits it to interested parties, without the users being aware. Types of information gathered can include: the websites visited, browser and system information, the computer IP address, as well as more sensitive information such as e-mail addresses, and passwords. Additionally, malware can cause browser hijacking, in which the user's browser settings are modified without permission. The software may create desktop shortcuts, display advertising pop-ups, as well as replace existing home pages or search pages with other pages.
10. Cyber Pornography: Cyber-pornography is the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials, especially materials depicting children engaged in sexual acts with adults. Cyber-pornography is a criminal offense, classified as causing harm to persons.
11. Password Sniffing: Password sniffers are able to monitor all traffic on areas of a network. Crackers have installed them on networks used by systems that they especially want to penetrate, like telephone systems and network providers. Password sniffers are programs that simply collect the first 128 or more bytes of each network connection on the network that's being monitored. When a user types in a user name and a password--as required when using certain common Internet services like FTP (which is used to transfer files from one machine to another) or Telnet (which lets the user log in remotely to another machine)--the sniffer collects that information.
12. Social-Hi-Jacking: This is a major crime all over the world. Many social networking pages have been hi-jacked by hackers who demands money in turn for releasing the personal social page. This has occurred in sites like Twitter, Facebook and Instagram. These fraudsters go as far as sending messages from the authorized page to friends and family re-questing for money or any other kind of assistance.

Also, another common scenario also occurs when the fraudster creates a social page pretending to be someone else especially celebrities.

13. Information Piracy and Forgery: Digital technology permits perfect reproduction of the original documents, examples are birth certificates, passport, false identity, counterfeiting of currency, negotiable instruments etc.
14. Cyber-Plagiarism: Information housed on the internet has made an effective alteration on the methods in which people educate themselves. The term 'Copy and Paste' is the most common phrase used when referring to cyber-plagiarism. Cyber-plagiarism can be defined as copying and pasting online sources into word processing documents without reference to the original writer /owner. In the educational sector in Nigeria, students, particularly those in the tertiary institutions carry out this crime without enforcing the due penalty.
15. Spam: Spam is the use of electronic messaging systems to send unsolicited bulk messages indiscriminately. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, online classified ads spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social networking spam, television advertising and file sharing network spam. Some of these address harvesting approaches rely on users not reading the fine print of agreements, resulting in them agreeing to send messages indiscriminately to their contacts. This is a common approach in social networking spam such as that generated by the social networking site (Saul, 2007).
16. Hacking: Information theft from computers hard disk, removal storage etc. Data theft, data destroy, stealing and altering information.
17. Drug Trafficking Deals:Another type of Cyber Crime is Drug Trafficking; it is a global trade involving cultivation, manufacture, distribution and sale of substances which are subject to drug prohibition law. Drug traffickers are increasingly taking advantage of the Internet to sell their illegal substances through encrypted e-mail and other Internet Technology. Some drug traffickers arrange deals at internet cafes, use courier Web sites to track illegal packages of pills, and swap recipes for amphetamines in restricted-access chat rooms.
18. Hate/Communal Crimes: As building a web page is not expensive and reaches to billions of people, criminals spread hate or communal information or rumors, by building a website and also recruits people for their operation through advertisement.
19. Altering Websites: The hacker deletes some pages of a website, uploads new pages with the similar name and controls the messages conveyed by the web site.

Prevention of Cyber Crime

Prevention is always better than cure. It is always better to take certain precaution while operating the net. A should make them his part of cyber life. Sailesh kumar Zarkar, technical advisor and network security consultant to the Mumbai Police Cybercrime Cell, advocates the 5P mantra for online security: Precaution, Prevention, Protection, Preservation and Perseverance. A netizen should keep in mind the following things:

1. To prevent cyber stalking avoid disclosing any information pertaining to one self. This is as good as disclosing your identity to strangers in public place.
2. Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.
3. Always use latest and update antivirus software to guard against virus attacks.
4. Always keep back up volumes so that one may not suffer data loss in case of virus contamination.
5. Never send your credit card number to any site that is not secured, to guard against frauds.
6. Always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children.
7. It is better to use a security program that gives control over the cookies and send information back to the site as leaving the cookies unguarded might prove fatal.

8. Web site owners should watch traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers may do this.
9. Use of firewalls may be beneficial.
10. Web servers running public sites must be physically separate protected from internal corporate network.

IT solutions to cybercrime

In almost all the developed countries, there is a central database that has details of all citizens and has links to other databases such as the car registration database held at the driver's vehicle licensing agency and to another powerful computer running the automated fingerprint identification system. Also same thing has been applicable to foreigners in the developed countries in which all foreigner fingerprints, and international passport numbers is inside the database, this integrated system helps in tracking down and controlling crime (Milhorn, 2007).

Except crime uncovering and deterrence are antagonized communally, Nigeria like any other country will have to continue genuine breeding grounds for cartels of such criminal actions. According to Ribadu (2007) A number of crime control and prevention initiatives have been implemented with the use of modern technology. Unfortunate the nation is not well equipped with sophisticated hardware to track down the virtual forensic criminals. Laura (2012) state that "African countries have been criticized for dealing inadequately with cybercrime as their law enforcement agencies are inadequately equipped in terms of personnel, intelligence and infrastructure, and the private sector is also lagging behind in curbing cybercrime" Nigeria is not an exception to this rule. Furthermore, it is therefore paramount that the nation's legislation should ensure proper implementation of their laws against cybercrime.

Beyond these however, more effort should be made to refocus on the promotion of positive uses of IT. In this regard, it is encouraging that Microsoft has partnered with an NGO (Paradigm Initiative Nigeria (PIN)) to tackle cybercrime through its Internet Safety, Security and Privacy Initiative for Nigeria (ISSPIN). The program essentially focuses on redirecting the energy of young Nigerians away from cyber-crime and towards positive utilization of cyber space for legitimate purposes. Microsoft also aims at addressing the need for adequate training in information technology among young Nigerians by distributing free compact discs containing Microsoft's Digital Literacy Curriculum. There is also the practical aspect of empowerment through training programs designed to arm youths with marketable skills for legitimate business activities in the online environment. As awareness continues to rise about the potentials of the technology, there is a corresponding need for the creation of local content online, establishment of websites for businesses, as well as online advertisements and marketing. Expertise and skills in these areas are therefore increasingly becoming more valuable, and a legal framework that deals with protection of creativity, prevention of misrepresentations and fraudulent acts become relevant. Hopefully, skill acquisition in these areas will not only reduce the tendency towards commission of cybercrimes, but also contribute to a reduction in the number of the unemployed in the country.

In banking sector, according to Aribake (2015) IT tools such as Transaction Authorization Code (TAC) and Password Electronic Token, user identification, SMS (short message services) alert, internet bank transfer, and bill payment, all these are the mainstream pre-emptive procedures used by the online banking in the Nigeria society to combats cybercrime in the banking sector. Transaction authorization code (TAC) is the consent code make available by the card issuer to the supplier at the time of the transaction (Cheng, Lam, and Yeung, 2006). It is convenient to use TAC in an online banking transactions, the cardholders getting to the transaction access code into the keypad of the card sources are authentically making use of card to exhibit a figure identical to the transaction consent code make available by the issuer. The authorization code and the equivalent consent code can be used to validate a card transaction to additional relief in fraud deterrence. TAC enables you to feel secure using it in your online banking transaction (Yiu, Grant and Edgar, 2007). TAC is always in a distinctive security code of 6-digit number use for registration &reset connect, online account settings and maintenance, specific online banking transaction. Token can be referred to as a device in which an authorized user of computer services is given to for comfort authentication. Token is being use to prove one's self with the aid of electronic means, using token prevent me from cyber fraud (Yiu, Grant

and Edgar, 2007). Token is being use in tallying to or in place of a password to verify that the customers is who they assertion to be. Token can be in two types: Hardware token & Software token. We have two elective inputs to token: Token input data & Token activation data. There are also some ways out in averting online banking crime such as: Protecting antivirus & firewall, restricting the amount of personal information one permit to be in public domain, making use of low limit distinct credit card for online buying to minimize the possible loss of things go wrong (Liao and Cheung, 2008).

Mugari, Gona, Maunga and Chiyambiro (2016) in their study identified education and training through seminars andworkshops, tight IT security, constant change of ICT technology to meet up with the changes, installation and constantupdating of security measures such as anti-viruses, protection of the banking sector through access control measures, installation of biometric security and use of smart cards. firewalls and firewalls data recovery sites. These all fall under thethree broadways to overcome cybercrime which are cyber laws, education and policy making as suggested Saini and Rao (2012). They also suggested separating critical banking applications from the web through firewalls. This was in support of the study by Siddique & Rehman (2011) which recommended the following protection measures; hardware identification, access control software and disconnecting critical banking application from the web.
Ibikunle and Eweniyi (2013) in their study listed some IT solutions to internet and cybercrime to include:

- Interactive Voice Response (IVR) Terminals: This is a new technology that is reported to reduce charge backs and fraud by collecting a "voice stamp" or voice authorization and verification from the customer before the merchant ships the order.
- IP Address tracking: Software that could track the IP address of orders could be designed. This software could then be used to check that the IP address of an order is from the same country included in the billing and shipping addresses in the orders.
- Use of Video Surveillance Systems: The problem with this method is that attention has to be paid to human rights issues and legal privileges.
- Antivirus and Anti Spyware Software: Antivirus software consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software. Anti-spy wares are used to restrict backdoor program, Trojans and other spy wares to be installed on the computer.
- Firewalls: A firewall protects a computer network from unauthorized access. Network firewalls may be hardware devices, software programs, or a combination of the two. A network firewall typically guards an internal computer network against malicious access from outside the network.
- Cryptography: Cryptography is the science of encrypting and decrypting information. Encryption is like sending a postal mail to another party with a lock code on the envelope which is known only to the sender and the recipient.[20] A number of cryptographic methods have been developed and some of them are still not cracked.
- Cyber Ethics and Cyber Legislation Laws: Cyber ethics and cyber laws are also being formulated to stop cyber-crimes. It is a responsibility of every individual to follow cyber ethics and cyber laws so that the increasing cyber-crimes will reduce. Security software like anti viruses and anti-spy wares should be installed on all computers, in order to remain secure from cyber-crimes. Internet Service Providers should also provide high level of security at their servers in order to keep their clients secure from all types of viruses and malicious programs.
- Establishment of Programs and IT Forums for Nigerian Youths: Since the level of unemployment in the country has contributed significantly to the spate of e-crime in Nigeria, the government should create employments for these youths and set up IT laboratories/forum where these youths could come together and display their skills. This can be used meaningfully towards developing IT in Nigeria at the same time they could be rewarded handsomely for such novelty.

Recommendations

According to Omodunbi, Odiase, Olaniyan, and Esan (2016) collaborative efforts of individuals, corporate organization and government could go a long way reduce cybercrime to a minimal level. Firms should secure their networked information. Cybercrime cannot be easily and completely wiped out, but can be reduced. However, collaborative efforts of individuals alongside with government intervention could go a long way to minimize it to a reasonable level. Measures to take can be categorized into two (Maitanmi, 2013):

1. Governments intervention: Although the country has found herself in great mess by the inability of the government to provide basic necessary amenities such as jobs, security and the likes for her citizens which indirectly has led to high rate in cybercrime, there is still need for the nation to come up with adequate laws to tackle this issue. These laws should be formulated by the government and should strictly be adhered to. However, it is worthy to note that a bill was recently passed in year 2015 that would protect and punish electronic fraud and other cyber related crimes. The full implementation of this bill will hopefully bring a strategic approach to fight against cybercrime. Some of the bills are highlighted below:

- There will be seven years' jail term for offenders of different types of computer related fraud, computer related forgery, cyber-pornography, cyber-stalking and cyber-squatting.
- Defines the liability of service providers and ensures that the use of electronic communications does not compromise national interest. It provides a legal framework to punish cyber criminals thereby improving electronic communication.
- It specifies all criminal acts and provides guidelines for the investigation of such offences. If these laws are effectively enforced, cybercriminals will be deterred and penalized. This will indirectly reduce the incident of cyber-crimes, increase customer's confidence while transacting business online and also correct the negative impression about Nigeria and the citizens.
- Individuals on their part should ensure proper security controls and make sure they install the latest security up-dates on their computer systems. In addition, they should observe the following (Lakshmi, 2015):
  - Carefully select the sites you visit. Do not visit an un-trusted site. Avoid visiting a site by clicking on a link you find in your email, found on a Facebook page, or on an advertisement.
  - Avoid pirated software and never disclose your Personal Identification Number (PIN), bank account and email access code to unknown persons.
  - Always ignore any e-mail requiring your financial in-formation. Do not send sensitive information in an email since its security cannot be guaranteed.
  - Use strong passwords that are difficult to guess and employ a combination of characters (upper case and lower-case letters), numbers and symbols.
  - Avoid inputting your information in a pop-up. If you have interest in any offer you see on a pop up, it is al-ways safer to go directly to the website of the retailer.
- Different professional bodies like Nigerian Computer Society (NCS) and Computer Professionals of Nigeria (CPN) could partner with government agencies like Nigeria, Communications Commission (NCC), National information Technology Development Agency (NITDA) among others to create awareness and sensitize the Nigerian people on the menace of cybercrime and ways to avoid them. Organizations, companies, firms and institutions that work with the internet and technological devices should take measures to protect themselves from attacks(Olanrewaju and Adebiyi, 2014).
- The network operators like MTN, Glo, Etisalat and Airtel should help to sensitize people and put in place policies to safeguard their clientele from attacks. Also, it is paramount they readily cooperate with law enforcement agencies when such crimes are reported and being investigated. To prevent cybercrime committed through calls placed from mobile phones and smart devices, Network operators could develop a system that would request for user authorization before a call is allowed. This system would enable each registered user to create and change a Personal Identification Number (PIN) that would be required before a call connects and the account balance subsequently debited. This means

that an unauthorized call cannot be placed from one's mobile number to perpetrate any crimes to implicate other individuals (Olanrewaju and Adebiyi, 2014).

- The traditional provisions on impersonation and criminal fraud as contained in Nigerian Criminal Code, Penal Code and AFF Act 2006 should be updated adequately take care of complex cases of phishing, identity theft and other electronic related economic crimes. At the moment, some of the legislative frameworks we have in the country have not been enacted, including the EFCC Act of 2010, sponsored by Hon. Abubakar. Even before the EFCC Amendment Act of 2010, there were some other bills that were also drafted and have been sent to the National Assembly, part of which has not yet been enacted as well. In 2005, there was the Computer Security and Critical Infrastructure protection bill sponsored by another law maker, that bill has never being enacted. In 2008, the Cyber Security Agency bill was sponsored by Hon. Bassey Etim, and has not been enacted and others like that which have not been enacted. There is therefore serious need for the law-makers to amend the EFCC Act for them to be able to arrest and prosecute cyber criminals in the most effective way (Ebeleke, 2011).

Conclusion

Nigeria been a third world nation is confronted with diverse of challenges for instances corruption, unemployment, poverty, and so on, making crime a thrive. The country is ranked third in global internet crime. It is true that Technology gives rise to cyber crime, the battle against cybercrime is also encouraged by IT security system. Therefore information technology security tools must come into play be addressed seriously as it is affecting the image of the country in the outside world.

References

Adomi, E. E. 92008). Security and software for cybercafes. DOI: 10.4018/978-1-59904-903-8

Akinsuyi (2009). The drawing of Information Security Legislations, What

Aribake, Fadare. O (2015). Impact of ICT tools for Combating Cyber Crime in Nigeria Online Banking: A conceptual Review. *International Journal of Trade, Economics and Finance. 6(5).*

Burden, K, Palmer, C and Lyde, B (2003), 'Cyber-Crime: A New Breed of Criminals?', 19(3) Computer Law and Security Report, 222.

Cheng, T. C. E., Lam, D. Y. C & Yeung. A. C. L. (2006). "Adoption of internet banking: an empirical study in Hong Kong," *Decision Support System 2006*, vol. 42, no. 3, pp. 1558–1572.

Council of Europe (COE), (2001). Convention on Cybercrime http://conventions.coe.int.

Critcher, (2003). Cybercrime and society

Ebeleke, Emmamuel (2011). Why cybercrime thrives in Nigeria, byEwelukwa; Vanguard News,http://www.vanguardngr.com/2011/04/why-cyber-crime-thrives-innigeria- by-ewelukwa/retrieved May 5, 2014

Ekoa, R. & Mungwe, M. (2018). A review of Cybercrime in Sub-Saharan Africa: A Study Cameroon and Nigeria. International Journal of Scientific & Engineering Research. 9(5) Retrieved from https://www.ijser.org/researchpaper/A-review-of-Cybercrime-in-Sub-Saharan-Africa-A-Study-Cameroon-and- Nigeria.pdf (Accessed: 12/10/2018).

Hassan, A. B., Lass, F. D. & Makinde, J. (2012). Cybercrime in Nigeria: Causes, Effects and the Way Out. *ARPN Journal of Science and Technology. 2(7), http://www.ejournalofscience.org*.

Ibikunle, Frank &Eweniyi, Odunayo (2013). Approach To Cyber Security Issues In Nigeria: Challenges And Solution. *(IJCRSEE) International Journal of Cognitive Research in science, engineering and education, 1(1).* www.ijcrsee.com.

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

Lewis, B. C (2004), 'Prevention of Computer **Crime** amidst International Anarchy', 41 American Criminal Law Review, 1353.

Liao, Z & Cheung, M. T (2008). "Measuring customer satisfaction in internet banking; A core framework," *Communications of the ACM*. 51(4) pp. 47-51.

Lininger, R and Dean, R (2005), Phishing, Cutting Identity Theft Line (Toronto: Wiley).

Littlewood, Anne (2003). Cyberporn and moral panic: an evaluation of press reactions to pornography on the internet.

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

Mbaskei, Martin Obono (2008): Cybercrimes: Effect on Youth Development http://www.i-genius.org accessed 26 the April 2012.

Milhorn, H. (2007). *Cybercrime: How to Avoid Becoming a Victim by True Crime*.

Mugari, I., Gona, S., Maunga, M & Chiyambiro, R. (2016). Cybercrime - The Emerging Threat to the Financial Services Sector in Zimbabwe. *Mediterranean Journal of Social Sciences MCSER Publishing, Rome-Italy Vol 7 No 3.*

Olanrewaju, O. M. & Adebiyi, F. O. (2014). The Impact of Mobile Information and Communication Technology on Cybercrime in Nigeria. *International Journal of Engineering Research & Technology (IJERT), 3 (8)* IJERTIJERT

Omodunbi, B. A., Odiase, P. O., Olaniyan, O. M. and Esan, A. O (2016).Cybercrimes in Nigeria: Analysis, Detection and Prevention. *FUOYE Journal of Engineering and Technology*, 1(1).

Poonia, A. S., Bhardwaj, A & Dangayach, G. S. (2011). Cyber Crime: Practices and Policies for Its Prevention. The First International Conference on Interdisciplinary Research and Development, 31 May - 1 June 2011, Thailand.

Ribadu, E. (2007). "Cyber crime and commercial fraud; A Nigerian perspective," presented at the Modern Law for Global Commerce, Vienna, 200

Saini, H., Rao, Y. S, & Panda, T. C (2012). Cyber-crime and their impacts: A Review International Journal of Engineering Research and Applications: vol 3, issue 2, pp. 202-209.

Saul, Hansell (2007):Social network launches worldwide spam campaign New York Times

Sesan, G. (2010). The New Security War. [Online]. Available: http://www.pcworld.com/article/122492/the_new_security_war.htm#tk.mod-rel

Siddique, M. I., Rehman, S. (2011). Impacts of Electroniccrime in Idian Banking Sector.

Siegel, Saukko, P. & Knupfer (2000). Overlapping cirminal offences and gendered. http://open.library.ubc.ca>pdf

Vladimir, G. (2005). International cooperation in fighting cybercrime. [Online]. Available: http://www. crimeresearch.org.

Webster, (2003). Making sense of the information age: sociology and cultural studies… http://www.tandfoline.com>doi>abs

Yiu, C.S., Grant, K. & Edgar, D (2007). "Factors affecting the adoption of internet banking in Hong 1020 Kong — implications for the banking sector," *Int J Inform Manage*, vol. 27, pp. 336–351, 2007.