ARPN Journal of Science and Technology

http://www.ejournalofscience.org

Cybercrime in Nigeria: Causes, Effects and the Way Out

[1] Anah Bijik Hassan, [2] Funmi David Lass, [3] Julius Makinde
[1, 2, 3] Faculty of Science and Technology, Computer Science Department,
Bingham University, Karu. Nasarawa State. Nigeria
[1] annebjk@binghamuni.edu.ng, [1] annebjk@yahoo.com
[2] dflass@yahoo.com
[3] julius.m@binghamuni.edu.ng, [3] juliusmakinde@yahoo.com

ABSTRACT

Cybercrime involves using computers and Internet by individuals to commit crime. Cyber terrorism, identity theft and spam are identified as types of cybercrimes. The study identified some of the causes of cyber crimes to include urbanization, unemployment and weak implementation of cyber crime laws. The effects of cybercrimes on organizations, the society and the country in general include reducing the competitive edge of organizations, waste of production time and damage to the image of the country. With Nigeria venturing into cashless society, there is a need for cybercrimes menace to be minimized if not completely eradicated. Some of the ways of combating such crimes include taking reasonable steps to protect ones property by ensuring that firms protect their IT infrastructure like Networks and computer systems; government should assure that cyber crime laws are formulated and strictly adhered to and individuals should observe simple rules by ensuring antivirus protection on their computer systems.

Keywords: *Cybercrimes, Nigeria, terrorism, fraud and spam.*

1. INTRODUCTION

Cyber Crime is one of the words frequently used by individuals in our contemporary Society. To understand the true meaning of cybercrime, there is the need to understand the slit meaning of Cyber and Crime. The term “Cyber” is a prefix used to describe an idea as part of the computer and Information age and “Crime” Can be described as any activity that contravenes legal procedure mostly performed by individuals with a criminal motive. Cybercrimes are defined as: "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, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones” Halder & Jaishankar (2011). Such crimes may threaten a nation’s security and financial health Saul (2007). Cyber crime can simply be explained as crimes carried out with the aid of a computer system.

The internet has offered a lot of platform for useful research purposes; However, Cyber crime is a worldwide problem that's costing countries billions of dollars. According to crime-research.org, as early as 2003 the United States was already leading the world in percentage of cyber attacks at 35.4 percent, followed by South Korea at 12.8 percent. Countries with high rates of computer piracy, such as Russia, have reacted slowly to cyber crime. As a result, many hackers and other cyber criminals can flourish in countries with few Internet crime laws while attacking richer countries through their computer because it lacks rules and codes of a central authority which governs it as such internet has no geographical demarcation as remarked by Guillane and Fortinet (2009).

In Nigeria, cyber crimes are perform by people of all ages ranging from young to old, but in most instances the young. Several youth engage in cyber crime with the aim of emerging as the best hacker, or as a profit making venture since the tools for hacking in our modern world has become affordable by many. Mbaskei 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. This study tends to look at Cybercrime, its causes, effects and suggests ways to combat such crimes as it affects Nigeria.

2. TYPES OF CYBER CRIMES

Cyber crimes simply put are crimes that are committed using the Computers and Networks. There are several types of cyber crimes some of which include:

a. 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. According to Wikipedia, a cyber terrorist is someone who intimidates a government or to advance his or her political or social objectives by launching computer-based attack against

ARPN Journal of Science and Technology

computers, network, and the information stored on them. For instance, a rumor on the Internet about terror acts. In addition, Parker (1983) defined Cyber terrorism as an act of terrorism committed through the use of cyberspace or computer resources. 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.

b. 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.

c. 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. The rise in Internet drug trades could also be attributed to the lack of face-to-face communication. These virtual exchanges allow more intimidated individuals to make comfortably purchase of illegal drugs. (www.wikipedia.com).

d. Malware

Malware refers to viruses, Trojans, worms and other software that gets onto your computer without you being aware it's there. Back in the early part of the century, most such software's primary aim was thrill. The people writing the software found it amusing to write a program that exploited security flaws just to see how far it could spread. Today the incentive for making such software is generally more dangerous. 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. 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.

e. Cyber Stalking

Cyber stalking is essentially using the Internet to repeatedly harass another person. This harassment could be sexual in nature, or it could have other motivations including anger. People leave a lot of information about themselves online. Such information can leave one vulnerable to cyber stalking, a term that essentially refers to using the Internet to stalk (to illegally follow and watch somebody), Justin (2010). Whereas content may be offensive in a non-specific way, harassment directs obscenities and derogatory comments at specific individuals focusing for example on gender, race, religion, nationality, sexual orientation. This often occurs in chat rooms, through newsgroups, and by sending hate e-mail to interested parties. (www.wikipedia.com)

f. 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).

Spamming remains economically viable because advertisers have no operating costs beyond the management of their mailing lists, and it is difficult to hold senders accountable for their mass mailings. Because the barrier to entry is so low, spammers are numerous, and the volume of unsolicited mail has become very high. A person who creates electronic spam is called a spammer, Gyongyi(2005).

ARPN Journal of Science and Technology

http://www.ejournalofscience.org

Wiretapping/Illegal interception of telecommunication

There are a number of ways that physical methods can breach networks and communications, for instance, if telephone and network wiring is often not protected as well as it should be, both from intruders who can physically damage it and from wiretaps that can pick up the data flowing across the wires. Criminals sometimes use wiretapping methods to eavesdrop on communications. It's unfortunately quite easy to tap many types of network cabling. For example, a simple induction loop coiled around a terminal wire can pick up most voices. Telephone fraud has always been a problem among crackers, but with the increasing use of cellular phones, phone calling cards, and the ordering of merchandise over the phone using credit cards, this problem has increased dramatically in recent years. Communications Security, it's important to physically secure all networks cabling to protect it both from interception and from vandalism. It has been reported that the notorious American hacker Kevin Poulsen was able to gain access to law enforcement and national security wiretap data prior to his arrest in 1991 (Littman 1997). In 1995, hackers employed by a criminal organization attacked the communications system of the Amsterdam Police. The hackers succeeded in gaining police operational intelligence, and in disrupting police communications (Rathmell, 1997).

g. Logic Bombs

A typical logic bomb tells the computer to execute a set of instructions at a certain date and time or under certain specified conditions. The instructions may tell the computer to display “I gotcha” on the screen, or it may tell the entire system to start erasing itself. Logic bombs often work in tandem with viruses. Whereas a simple virus infects a program and then replicates when the program starts to run, the logic bomb does not replicate – it merely waits for some pre-specified event or time to do its damage. Time is not the only criterion used to set off logic bombs. Some bombs do their damage after a particular program is run a certain number of times. Others are more creative. There are several reported cases that a programmer told the logic bomb to destroy data if the company payroll is run and his name is not on it.; this is a sure-fire way to get back at the company if he is fired! The employee is fired, or may leave on his own, but does not remove the logic bomb. The next time the payroll is run and the computer searches for but doesn’t find the employee’s name, it crashes, destroying not only all of the employee payroll records, but the payroll application program as well. Logic bombs present a major threat to computer systems, not just because of the damage they themselves can do, but because they provide a technique to facilitate more devastating crimes.

h. 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. Additional programs sift through the collected information, pull out the important pieces (e.g., the user names and passwords), and cover up the existence of the sniffers in an automated way. Best estimates are that in 1994 as many as 100,000 sites were affected by sniffer attacks. (David et al, 1995)

3. CAUSES OF CYBER CRIME IN NIGERIA

The Nigerian population census in 2006 reveals that Nigeria is a country with about 160 million people. This write up discusses some of the reasons that may cause cyber crime in Nigeria

a. Urbanization

Urbanization is one of the causes of Cyber crime in Nigeria; it is the massive movement of people from rural settlement to Cites. According to Wikipedia urbanization is looked at as the massive physical growth of urban areas as a result of rural migration in search for a better life. This result in a heavy competition amongst the growing populace more especially the elites, as such the elites find it lucrative to invest in the crime of cyber because it is a business that requires less capital to invest and they are popularly called “Yahoo Boys”. Meke (2012), in his article “Urbanization and cyber crime in Nigeria” reiterated urbanization as one of the major causes of cyber crime in Nigeria and Urbanization will be beneficial if and only if good jobs can be created in the cities where population growth is increasing, in his article, he emphasized that urbanization without crime is really impossible. As such the elites amongst them find it lucrative to invest in the cyber crime because it is a business that requires less capital.

b. Unemployment

Cybercrime can be associated with high rate of unemployment, harsh economic conditions, and poor educational system. According to the Nigerian National Bureau of Statistics, Nigeria is saddled with almost 20 million unemployed people, with about 2 million new

ARPN Journal of Science and Technology

http://www.ejournalofscience.org

entrants into the dispirited realm of the unemployed each year. This clearly reveals that a lot of youths are not employed. There is an adage that says "an idle mind is the devils workshop", as such most of our youth will use their time and knowledge as a platform for their criminal activity, in order to improve their livelihood and to make ends meet.

c. Quest for Wealth

Another cause of cyber crime in Nigeria is quest for wealth, there exist a large gap between the rich and the average, as such many strive to level up using the quickest means possible, since for any business to thrive well, the rate of return in the investment must be growing at a geometric rate with a minimal risk. Most cyber criminals require less investment and a conducive environment. Nigeria is such an environment and many cyber criminals take advantage of that.

d. Weak Implementation of Cyber Crime Laws and Inadequate Equipped Law Agencies

The Nigerian legislation must implement strict laws regarding cyber criminals and when criminal offences occur, perpetrators must be punished for the crime they've committed because cyber crimes reduces the nation's competitive edge, failure to prosecute, cyber criminals, can take advantage of the weak gaps in the existing penal proceedings. Weak /fragile laws regarding cyber criminals exist in Nigeria, unlike in the real world were criminals such as armed robbers are treated with maximum penalties. 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 cyber crime.

e. Negative Role Models

Youths are mirrors of the society, but it is quite unfortunate how parents neglect their rightful duties. Meke (2012) remarked that today many parents transmits crime values to their wards, via socialization as if it a socio cultural values which ought to be transmitted to the younger generation. Imagine a situation where the child supplies the father with vital information to wreck individual's banks account using the computer system, while the mother impersonates the account holder/owner at the bank. If this culture is imbibed among the younger generations most of them will see no wrong in cyber crime practices.

4. EFFECTS OF COMPUTER CRIME

a. Reduces The Competitive Edge Of Organizations

Computer crimes over the years have cost a lot of havoc to individuals, private and public business organization within and outside the country, causing a lot of financial and physical damage. Due to cyber crime, there has being loss of billions of dollars annually globally speaking, such crimes may threaten a nation's security and financial health, a company can suffers losses due to computer crime when a hacker steals confidential information and future plans of the company. And he simply sells the information to a competitor company; this will automatically reduce the competitive strength of the company.

b. Time Wastage And Slows Financial Growth

Wastage of time is another problem because many IT personals may spend a lot of time on handling, rectifying harmful incidents which may be caused by computer criminals. The time spent should have earned a profit to the organization. One peculiar problem is that, when a hacker enter in an organization and steals confidential information from the company the people who entrust the company loses their confidence in the company as the company may contains confidential information like credit cards of customers and as the information is stolen the customer will not trust the company again and will move to someone else who could protect their confidential information.

c. Slows Production Time and Add to Over Head Cost

Computer crime reduces the productivity of a company, as a company will take measure to reduce cybercrime, by entering more password or other acts this will take time to do and therefore will affect productivity. Computer crime will increase the cost as to stop viruses and malware companies must buy strong security software to reduce the chances of attacks from such attacks.

d. Defamation Of Image

With high level of cyber crime in the nation, the slogan "GOOD PEOPLE GREAT NATION"by Nigerians will be tarnished and global community will view the other side of the coin. Other effects includes the consumption of computer and network resources, and

ARPN Journal of Science and Technology

the cost in human time and attention of dismissing unwanted messages

5. COMBATING CYBER CRIME IN NIGERIA

Cybercrime cannot be easily and completely eliminated, but can be minimized. However, collaborative efforts of individuals, corporate organization and government could go a long way reduce it to a minimal level. Firms should secure their networked information. Other measures to e taking include:

1. Laws to enforce property rights work only when property owners take reasonable steps to protect their property in the first place. As one observer has noted, if homeowners failed to buy Locks for their front doors, should towns solve the problem by passing more laws or hiring more Police? Even where laws are adequate, firms dependent on the network must make their own Network, Information and computer systems secure. And where enforceable laws are months or years away, as in most countries like Nigeria, this responsibility is even more significant.

2. Governments should assure that their laws apply to cybercrimes.

African countries are bedeviled by various socio-economic problems such as poverty, AIDS, fuel crisis, political and ethnic instability and other related crimes. This limits their strength to effectively combat cyber crime. Nevertheless, it is important that Nigeria as a nation take measures to ensure that its penal and procedural law is adequate to meet the challenges posed by cybercrimes. The Government must ensure laws are formulated and strictly adhered to.

3. Individuals should observe simple rules

Individuals on their part should ensure proper anti-malware protection on their computer systems, individuals should be encouraged to avoid pirated software, never to share their Personal Identification Number(PIN), bank account, email access code to unknown persons, never disclose any confidential information to anybody as none of these networks were design to be ultimately secure. Ignore any e-mail requiring any financial information. Report particularly evil spam to the appropriate authorities as suggested by Justin (2010). Mbasekei (2008) suggested that Telecommunication Regulatory Agencies should enhance security on internet service providers' server in other to detect and trace cybercrimes and creation of job opportunities for the teeming unemployed youths will go a long way in minimizing the menace.

6. CONCLUSION

For Nigeria to serve as a fertile ground for economic break through, it must be build on a crime free society. But an ideal economy is virtually not possible, because as technology increases so also crime rate. Cyber criminals will always keep in pace with any technological advancement. It is true that Technology gives rise to cyber crime. The future of our economy lies in our hands, the future itself is the summation of our decisions so we should believe in ourselves and endeavor to do the right thing at each point in time, following carefully the suggestions of this paper. Until then, the dreamed society will not become a reality.

References

[1] Halder, D., & Jaishankar, K. (2011): Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9.

[2] Saul Hansell(2007):Social network launches worldwide spam campaign New York Times

[3] Guillaume Lovet Fortinet, (2009): Fighting Cybercrime: Technical, Juridical and Ethical Challenges VIRUS BULLETIN CONFERENCE.

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

[5] Parker D (1983): Fighting Computer Crimes, U.S. Charles Scribner's Sons.

[6] Http:// www.wikipedia.com.

[7] Malware (2012): www.wikipedia.com. Accessed on 09/07/ 2012 by 9:00 am prompt.

[8] Justin Plot (2010): Top five computer crime and how to protect yourself from them, Publication of Justin plot

[9] Littman, J. (1997): The Watchman: The Twisted Life and Crimes of Serial Hacker Kevin Paulsen. Boston: Little Brown.

[10] Rathemell, A. (1997): Cyber-terrorism: The Shape of Future Conflict? Royal United Service Institute Journal

[11] Meke Eze Stanley, N. (2012): An article "Urbanization and Cyber Crime in Nigeria: Causes and Consequences".

ARPN Journal of Science and Technology

[12] Laura Ani (2011): "Cyber Crime and National Security: The Role of the Penal and Procedural Law

[13] Mbaskei Martin Obono (2008): Cybercrimes: Effect on Youth Development, http://www.i- genius.org