Original Article

THE ROLE OF ICT IN COMBATING CYBERCRIMES: A STUDY FROM ABRAKA, DELTA STATE, NIGERIA

Olumide Bola Adebayo

Department of Library & Information Science, Delta State University
Abraka, Delta State, Nigeria
DOI: https://doi.org/10.5281/zenodo.14859974

Abstract: This study investigated Information and Communication Technology (ICT) and its impact in combating cybercrimes in Abraka, Delta State as a case study. In order to achieve the purpose of this study, questionnaire was used to elicit information from the respondents. The sample size for the study is one hundred and five (105), which constituted 10% of the entire population. The data collected were critically analyzed and the major findings revealed the following: that yahoo attack (also called 419) and hacking are the most prevalent cybercrimes in rural communities, that financial losses and abandonment of rural communities by government are the major impacts of cybercrime in rural areas, that unemployment and quest for wealth are the major cause of cybercrimes in rural communities. Finally, recommendations were made that control measures should be adopted by the various agencies concerned in order to curb cybercrimes in rural communities.

Keywords: Cybercrimes, ICT, Technologies, Rural Communities, Delta State, Nigeria

INTRODUCTION

The advent of digital technology gave birth to modern communication hardwares, internet service and powerful computer systems to process data (Hunda, Singh & Singh.
2014). Society‟s reliance on computer system has a profound human dimension. In recent years, computers and sharing of information have penetrated nearly every aspect of human life and offers gargantuan benefits to the society (Olumoye, 2013). This has also presented plenty of opportunities for anti-social and criminal behaviour in non-traditional ways. The rapid expression of large-scale computer networks with the ability to access many systems through regular telecommunication lines increase the vulnerability of these systems and the opportunity for misuse or criminal activity.

According to Matanmi, Ogunlere, Ayinde and Adekunle (2013), cybercrime began with disgruntled employees causing physical damage to the computers they worked with, aiming at getting back at their supervisors. But as

the ability to have personal computer at home became more accessible and popular, cyber criminals began to focus their efforts on home users (Matanmi, et al., 2013).

However, Taylor (2014: 13) defined cybercrime as:

"a criminal activity involving an information technology infrastructure: including illegal access or unauthorized access; illegal interception that involves technical means of non-public transmissions of computer data to, from or within a computer system; data interference that include unauthorized damaging, deletion, deterioration, alteration or suppression of computer data; systems interference that is interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data; misuse of devices, forgery (ID theft), and electronic fraud"

Cyber crime and technology misuse can be viewed as the result of the growing trend of society depending upon computer system and improving its use of technology. A computer system is just another tool and like other tools in the past which can be used for good or evil, and existing law is very likely to be unenforceable against these crimes (Ibikunle, 2005). More and more organizations and the society at large rely on the services and resources provided via the networks and computers. The organizations may depend on the data for their transactions, while individuals in the society may store information that is important for their personal or work related activities. The growing danger from crimes committed against computers, or information on computer is beginning to claim attention in national capitals in most countries around the world.

However, existing laws are likely to be unenforceable against such crimes. This lack of legal protection means that businesses and governments must rely solely on technical measures to protect themselves from those who would steal, deny access to valuable information (McConnell, 2010). Herselman and Warren (2013) sermonized that cybercrime has no borders or physical boundaries, it is also not subject to importation, customs or forex constraints thus making it a target by anyone from anywhere in the world (Herselman & Warren, 2013). Estimating the incidence, prevalence cost or some other measures of computer related crimes is a very difficult task because cybercrime cannot be quantified unlike some other criminal acts such as theft. This is also due to the fact that most critical crimes perpetuated are not detected, not even by their victims because disclosure of such crime could prove embarrassing or inconveniencing to victims.

As electronic commerce and online business become a part of today‟s business world, these types of issue becomes more important and more dangerous. Hacking and attacks are continually on the rise and companies are well aware of it (Olumoye, 2013). The legal system and law enforcement agents seem not to be keeping pace in tracking down cyber criminals and successfully prosecuting them in the law court. New technologies to fight these types of attacks are on their way, but there is need to be proper laws, policies and methods of actually catching the perpetrators and making them pay for the damage they cause (Albrecht, 2015).

Consequently, it become imperative to keep pace in tracking down computer related illegalities through policies, updated laws and methods of actually holding the perpetrators and making them to face the wrath of the law in order to protect the computer systems, networks and the data stored on them. Therefore, this study is aimed at investigating information and communication technology (ICT) use in combating cybercrimes in Abraka, Delta State as a case study.

Original Article

PURPOSE OF THE STUDY

The main purpose of the study is to investigate information and communication technology (ICT) use and its impact in combating cybercrimes in rural communities in Nigeria using Abraka, Delta State. The specific objectives of the study are to;

(i) identify the various types of cybercrimes most prevalent in Abraka, Delta State, Nigeria;

(ii) examine the effect of cybercrimes and technology misuse on the development of Abraka, Delta State;

(iii) investigate the causes of cybercrimes prevalence in rural communities in Nigeria; and (iv) Assess the control measures to curb cybercrimes in rural communities in Nigeria.

RESEARCH QUESTIONS

The following research questions were put forward to guide the study;

(i) What are the various types of cybercrimes most prevalent in Abraka, Delta State, Nigeria?

(ii) What are the effects of cybercrimes and technology misuse on the development of Abraka, Delta State?

(iii) What are the causes of cybercrimes prevalence in rural communities in Nigeria?

(iv) What are the control measures to curb cybercrimes in rural communities in Nigeria?

LITERATURE REVIEW

Cybercrime is any criminal offenses committed using the internet or another computer network as a component of the crime. They are offences that are committed against individual or group of individuals with a criminal motive to internationally 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 and mobile phones (Akogwu, 2012). Cybercrime is ever becoming prevalent in developing countries. In Nigeria, for example, the cyber criminals are being nick named the "yahoo boys".

Types of Cybercrimes most prevalent in Rural Communities in Nigeria

Cybercrimes simply put are crimes that are committed using the computers and networks. There are numbers of common attacks and methods of committing a cybercrime or computer related crime. Some of these methods may be less sophisticated than others and can be committed by someone with limited knowledge of computers while others may require programming skills; though these lists are not necessarily exhaustive (Olumoye, 2013). .

However, according to Hassan, Lass and Makinde (2012), there are several types of cybercrimes prevalent in Nigerian economy; some of which include: (1) 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 (Halder & Jaishankar, 2011). According to Wikipedia (2015), 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 computers, network, and the information stored on them. For instance, a rumor on the Internet about terror acts.

In addition, Hassan, Lass and Makinde (2012) citing 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 (Hassan, Lass and Makinde (2012).

(ii) **Fraud - Identity Theft**

Fraud is a criminal activity in which someone pretends to be somebody and retrieve vital information about someone (Hassan, Lass & Makinde, 2012). For instance, making a false bank webpage in order to retrieve information of the account of a client. 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 (Hassan, Lass & Makinde, 2012).

(iii) **Drug Trafficking Deals**

Another type of cybercrime 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).

(iv) Malware

Malware refers to viruses, Trojans, worms and other software that gets into your computer without you being aware it‟s there. Back in the early part of the century, most of 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 (Hassan, Lass & Makinde, 2012).

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 (Hassan, Lass & Makinde, 2012).

(v) **Cyber Stalking**

According to Hassan, Lass and Makinde (2012), 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).

(vi) **Spam**

Original Article

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 (Hassan, Lass & Makinde, 2012). 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 (Mbaskei, 2008).

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 (Mbaskei, 2008).

(vii) **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 (Hassan, Lass & Makinde, 2012).

(viii) 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 (Hassan, Lass & Makinde, 2012). The instructions may tell the computer to display "I gotcha" on the screen, or it may tell the entire system to start erasing itself.

Furthermore, Ehimen and Adekanle (2009) stated that 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 prespecified 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.

According to Hassan, Lass & Makinde (2012), 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 (Ehimen & Adekanle, 2009).

(ix) Password Sniffing

Original Article

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.

Laura (2011) posited that 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 usernames and passwords), and cover up the existence of the sniffers in an automated way.

Effect of Cybercrimes and Technology Misuse on the Development of Rural Communities in Nigeria

Cybercrime is a huge problem threatening technological advancement and the integrity of the internet as well as our personal lives (Olumoye, 2013). According to Olumoye, it has a tremendous impact on the society. The impact of a single attack can be very devastating, financial loses and theft of intellectual property. The overall monetary impact of cybercrime on government and individuals runs into billions of dollars.

Although, it is not every person who uses technology that utilizes it for negative purposes just as not every person uses it for good and knows the difference why or even cares. The fact of the matter is that technology has brought about many positive changes to the society. It is the peoples use or misuse of technology that is negative. Technology is being treated no differently than most other inventions throughout history (Kirk, 2008).

Cybercrime has a tremendous impact on the society, although as stated by Kirk (2008), cybercrime may not be violent in nature or is as readily noticeable as waking up and having your car missing from your drive way; its impact is severe and ultimately affects us all. The atrociousness of some of these cybercrimes is astounding and some of the figures are overwhelming (Kirk, 2008).

Moreover, not only do computer crimes harm the websites and people that are attacked, they also impact the software and service companies (e.g. Microsoft and Cisco) (Olumoye, 2013). Research shows that even the possibility of an attack can damage a software company due to vulnerability; out of eighteen (18) software suppliers surveyed there was a 0.6 percent fall in stock prices due to an announcement of vulnerability (Moffitt, Pannatia, Prosenbeck, Scott & Siversen, 2012).

In addition, the cyber criminals may see their actions as being victimless, but in the vicious cycle the entire society is affected by their wrong actions. Integrity of software program, company employees and customers are diminished because of cyber crimes and technology misuse. Trust is also lost between the seller and consumer. The loss in trust between sellers and consumers eventually affects the economy (Moffit et al., 2012).

Another impact as revealed by Olumoye (2013) is the usage of the web for sexual abuse. This has remained a very active research interest. Researchers have investigated the involvement of youths and children, who are involved with online sexual activities. These, researchers have spent time online in viewing sexual activities as a yardstick for measuring susceptibility to violent sexual conducts (Longe, Ngwa, Wada & Mbarika, 2009).

Causes of Cybercrimes Prevalence in Rural Communities in Nigeria

According to Matanmi, Ogunlere, Ayinde and Adekunle (2013), cyber crime began with disgruntled employees causing physical damage to the computers they worked with, with the aim to get back at their supervisors. But as

the ability to have personal computer at home became more accessible and popular, cyber criminal began to focus their efforts on home users (Matanmi et al, 2013).

However, some of the reasons that may cause cyber crime in Nigeria are classified by Matanmi et al., (2013) to include the following:

(a) Urbanization

Urbanization is one of the causes of Cyber crime in Nigeria. It is the massive movement of people from rural settlement to cities. 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" (Hassan, Lass & Makinde, 2012).

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, Meke 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 (Matanmi et al, 2013). According to the Nigerian National Bureau of Statistics, Nigeria is saddled with almost 20 million unemployed people, with about 2 million new 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 (Meke, 2012). 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 (Matanmi, et al., 2013).

(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 have 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 (2011) stated 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.

Original Article

Furthermore, it is therefore paramount that the nation‟s legislation should ensure proper implementation of their laws against cyber crime (Laura, 2011).

(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 (Matanmi et al, 2013).

Control Measures to Curb Cyber Crimes in Rural Communities

The foregoing points to the fact that it is imperative to curb the occurrences of cybercrimes in Nigerian economy. 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 to reduce it to a minimal level. Firms should secure their networked information. Preventive measures to be taken as posited by Hassan, Lass and Makinde (2012) 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, and never disclose any confidential information to anybody as none of these networks were design to be ultimately secure. Mbaskei (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.

Furthermore, in order to reduce cyber crime and technology misuse to the barest level if not entirely eliminated from our society, Olumoye (2013) recommended the following preventive measures:

(i) **Awareness and Training**

These are the first set of steps in alleviating cyber crimes. The citizens, consumers and organizations should create the awareness of cyber threats and the actions they can take to protect their information. Also, continuous training is necessary for business clients in order to share the responsibility in fighting against cyber crime.

Original Article

(ii) **Ethical and Moral Standards**

Ethical standards should be upheld in organizations to ensure confidentiality is served and technology misuses are reduced (Ibikunle, 2005). Computer ethnics help us to identify offenders and create solutions to aid in the minimization of computer crimes and technology misuse (Moor, 1985 cited in Olumoye, 2013).

(iii) **Computer Forensics**

Computer Forensics technically refers to the use of procedure centric approaches in the study of cyber-attack prevention, planning, detection and response with the goals of counteracting and conquering hacker attacks by logging malicious activity and gathering court admissible chains of evidence using various forensics tools that reconstruct criminally liable actions at the physical and logical levels (O‟ Connor, 2003).

According to Ibikunle (2005), an advanced computer forensics is the use of steganography, which is the art of hiding communications. Unlike encryption that uses an algorithm and a seed value to scramble or encode a message to make it unreadable; steganography makes the communication invisible. This takes concealment to the next level, which is to deny that the message even exists.

(iv) **Cyber Crime Prevention Laws**

According to McConnell (2000), National government remains the dominant authority for regulating criminal behaviour in most places in the world. If a nation has already struggled from and ultimately improved its legal authority after a confrontation with the unique challenge presented by cyber crime; it is crucial that other nations profit from this lesson and examine their current laws to discern whether they are composed in a technologically neutral manner that would not execute the prosecution of cyber criminals.

In many cases, nations will find that current laws ought to be updated. Enactment of enforceable computer crime laws that also respect the rights of individuals are an essential next step in the battle against this emerging threat (McConnell, 2000). The attacker sophistication seems to be ahead of defensive tools. That is the nature of the war between hacker and defenders; the attackers are always a step ahead. But by making the attackers‟ job harder and harder, and by increasing the length of gaol sentences for cyber crime and improving international police co-operation and skill levels, we can combine to keep up with the attackers and over time begin to turn the tide (Valacich & Schneider, 2010)

(v) **Encryption (or Cryptography)**

This involves scrambling data into an unreadable format called cipher text before it is transmitted over a telecommunication link between two computers, and then unscrambling that data again when it gets to its destination computer. Only those who possess the secret key can decipher (or decrypt) the message into plain text. If data is not encrypted during transmission, it can easily be intercepted by unauthorized party thereby making the third party to have access to the information. Encrypted messages can sometimes be broken by cryptanalysis, also called code-breaking; although modern cryptography techniques are virtually unbreakable. Cryptography is used to protect e-mail messages, credit card information and corporate data (Olumoye, 2013).

(vi) **Anti- Virus**

Anti-virus is a software program that is used to protect computer system against the menace of viruses. The effect of this software is to detect and remove a virus from a computer system before it does any damage to it. These software programs can readily be purchased from software stores or downloaded from the internet. Examples of

antivirus software are: Shield Deluxe, CA anti-virus, BitDefender, Avira, Kaspersky, Avast, Norton, NOD32, Dr. Solomon, MCAFFEE, MSAV and AVG.

(vii) **Firewall**

Firewalls are made up of software and hardware placed between an organization‟s internal and external networks to prevent outsiders from invading their networks. Firewalls are programmed to intercept and examine any message packet passing between the two networks and reject unauthorized messages.

(viii) **Passwords**

Passwords are unique set of characters that may be allocated to an individual, a particular system or facility that must be input to allow access. Passwords are security measure used by the majority of computer users which allows only authorized user to gain access to the system. The lack of password on a computer system increases the risk of unauthorized access. To prevent hackers and crackers from penetrating your network, it is recommended that you use passwords that are difficult to guess. It is better you make your passwords a mixture of letters, numbers and special characters such as: @, !, $, %, „, &, *, # etc. Moreover, you should always change your password at regular intervals and set a minimal length of passwords such as a minimum of six or eight characters (Olumoye, 2011).

RESEARCH METHODS

The survey research method was employed for this study. The research instrument used for the study is the structured questionnaire. The population of this study comprises of all the youths resident in Abraka, Ethiope East L. G. A. of Delta State which is estimated to be 1,057. The stratified random sampling procedure was adopted to arrive at the sample for the study whereby the researcher grouped the youths according to their occupation, social status and age. Thus, grouping the youths into strata, 10% was taken by the researcher, which resulted to 105 youths.

RESULTS AND DISCUSSIONS Demographic Variables

Table 1: Gender Distribution of the Respondents

Gender	Frequency	Percentage (%)
Male	75	71.4
Female	30	28.6
Total	**105**	**100**

The male respondents are 75 (71.4%) and their female counterparts is 30 (28.6%). This shows that there are more males than females that are involved in cyber crimes.

Table 2: Occupation Distribution of the Respondents

Occupation	Responses	Percentage (%)
Business	34	32.4
Farming	59	56.2
Studying	12	11.4
Total	**105**	**100**

34 (32.4%) of the respondents are into business, 59 (56.2%) are into farming while 12 (11.4%) respondents are studying.

Original Article

Table 3: Qualification Distribution of the Respondents

Educational Qualification	**Responses**	**Percentage (%)**
No Qualification	19	18.1
First School Leaving Certificate	73	69.5
OND/NCE	5	4.8
B.Sc./HND/BLS/B.A.	7	6.7
M.Sc./MLIS/M.A.	1	0.9
Ph.D	-	-
Total	**105**	**100%**

Table 4.4 discloses the educational qualification of the respondents. 19 (18.1%) of the respondents do not possess any qualification, 73 (69.5%) have First School Leaving Certificate (FSLC), 5 (4.8%) are OND/NCE holders, 7 (6.7%) respondents have B.Sc./HND/BLS/B.A. degree while only 1 (0.9%) respondent is a M.Sc./MLIS/M.A. degree holder. However, none of the respondents is a Ph.D holder. It is evident therefore that majority of the youths involved in cyber crimes are First School Leaving Certificate holders.

Research question one: What are the various types of cybercrimes most prevalent in Abraka, Delta State?

The data from research question one was presented in table 4.5

Table 4.5: Types of cybercrimes most prevalent in Abraka, Delta State

Types of Cybercrimes	**Agree**	**Percentage (%)**	**Disagree**	**Percentage (%)**
Yahoo Attack (also called 419) or YahooYahoo	105	100	0	0
Hacking	105	100	0	0
Credit Card / ATM Fraud	98	93.3	7	6.7
Fraud – Identity Theft	43	41	62	59
Drug Trafficking Deals	99	94.3	6	5.7
Software Piracy	37	35.2	68	64.8
Cyber Stalking	12	11.4	93	88.6
Wiretapping/Illegal interception of telecommunication	71	67.6	34	32.4
Password Sniffing	102	97.1	3	2.9
Virus Dissemination	104	99	1	1

Source: Field survey, 2016

Research question Two: What is the effect of Cybercrimes and Technology Misuse on the Development of Abraka, Nigeria?

The data from research question two was presented in table 4.6

Table 4.6: Effect of Cybercrimes and Technology Misuse on the Development of Abraka, Nigeria

Original Article

Impacts of Cybercrimes	**Agree**	**Percentage (%)**	**Disagree**	**Percentage (%)**
Financial losses	105	100	0	0
Theft of intellectual property	43	41	62	59
Sexual Abuse	98	93.3	7	6.7
Abandonment of rural communities by government	105	100	0	0
Loss of trust on youths	99	94.3	6	5.7

Source: Field survey, 2016

Research question Three: What are the causes of Cybercrimes prevalence in Rural Communities in Nigeria?

The data from research question three was presented in table 4.7

Table 4.7 Causes of Cybercrimes prevalence in Rural Communities

Causes of Cybercrimes	**Agree**	**Percentag e (%)**	**Disagree**	**Percentage (%)**
Urbanization	78	74.3	27	25.7
Unemployment	105	100	0	0
Quest for wealth	102	97.1	3	2.9
Weak implementation of cyber crime laws and inadequate equipped law agencies	39	37.1	66	62.9
Negative role models	94	89.5	11	10.5

Source: Field survey, 2016

Research question Four: What are the Control Measures to Curb Cyber Crimes in Rural Communities?

The data from research question four was presented in table 4.8

Table 4.8 Control Measures to Curb Cyber Crimes in Rural Communities

Cybercrimes Control Measures	**Agree**	**Percentage (%)**	**Disagree**	**Percentage (%)**
Governments at all levels should assure that their laws apply to cybercrimes	105	100	0	0
Ignore any e-mail requiring any financial information	102	97.1	3	2.9
Report particularly evil spam to the appropriate authorities	104	99	1	1
Individuals should observe simple rules on using the cyber space	101	96.2	4	3.8
Computer forensics	94	89.5	11	10.5
Encryption (or cryptography) of data	100	95.2	5	4.8

Source: Field survey, 2016

Original Article

DISCUSSION OF FINDINGS

In table 4.5, it is discovered that there are various types of cybercrimes most prevalent in Abraka, Delta State. Yahoo attack (also called 419) and hacking are the most prevalent cybercrimes in rural communities. However, Virus dissemination (99%), password sniffing (97.1%), drug trafficking deals (94.3%), credit card/ATM fraud (93.3%) and wiretapping/Illegal interception of telecommunication (67.6%) are also prevalent cybercrimes in rural communities. Cyber stalking, software piracy and identity theft were not considered too prevalent in Abraka. However, this analysis clearly shows that all the cybercrimes are prevalent in the rural community under study which is in line with Matanmi, Ogunlere, Ayinde and Adekunle (2013) who asserted that cybercrimes most prevalent in rural communities in Nigeria include yahoo attack, hacking amongst others.

In table 4.6, the results of the impacts of cybercrimes and technology misuse on the development of rural communities in Nigeria were disclosed. Financial losses and abandonment of rural communities by government are the major effects as noted by 100% of the respondents. 94.3% agreed that cybercrimes in rural communities results to the mistrust of youths. 93.3% agreed that sexual abuse was also an impact of cybercrime. 59% do not believe theft of intellectual property is an impact of cybercrime in rural communities in Nigeria. This analysis clearly supports the view of Kirk (2008) who opined that cyber crime has a tremendous impact on the society and Olumoye (2013) who asserted that the impact of cybercrimes on rural communities ranges from financial losses to health problems.

From table 4.7, the causes of cybercrimes prevalence in rural communities in Nigeria was discussed. Unemployment was seen as the major cause by 100% of the respondents. 97.1% blamed cybercrimes in rural communities on youth‟s quest for wealth. Also, 89.5% said negative role models contribute to the cause. 74.3% blamed urbanization. However, 62.9% did not agree to weak implementation of cyber crime laws and inadequate equipped law agencies as a cause of cybercrime prevalence in rural communities. These support the findings of Matanmi, et al., (2013) who opined that possible reasons that may cause cyber crimes in a society include unemployment amongst others.

Table 4.8 shows some of the control measures to adopt in order to curb cyber crimes in rural communities. 100% agreed that governments at all levels should ensure that their laws apply to cybercrimes, 99% agreed that evil spam should be particularly reported to the appropriate authorities, 97.1% agreed that e-mails requiring any financial information should be ignored, 96.2% affirmed that individuals should observe simple rules, 95.2% believes encryption (cryptography) of data will curb cybercrimes while 89.5% agreed to the use of computer forensics to fight cybercrimes. These findings are in accordance with the words of Olumoye (2013) who pointed out that in order to reduce cyber crime and technology misuse to the barest level, if not entirely eliminated from our society, preventive measures should be adopted.

CONCLUSION AND RECOMMENDATIONS

Based on the findings of this study, it can be seen that yahoo attack (also called 419) and hacking are the most prevalent cybercrimes in rural communities. This results into financial losses and abandonment of rural communities by government are the major effects of cybercrime in rural areas, since the perpetrators do this as a result of unemployment and quest for wealth. Control measures should be adopted by the various agencies concerned in order to curb cyber crimes in rural communities.

Therefore, the following are thus recommended:

- That a National Computer Crime Response Centre should be set up by the government which will comprise of experts and professionals to establish rules, regulations and standards of authentication of each citizen‟s records and staff of establishments, etc.
- Forensics commission should be established, which will be responsible for the training of forensics personnel
- Comprehensive laws to combat computer and cyber related crimes should be promulgated to fight cybercrimes in Nigeria.

REFERENCES

Akogwu, S. (2012). An Assessment of the Level of Awareness on Cyber Crime among Internet Users in Ahmadu Bello University, Zaria (Unpublished B.Sc. project).

Department of Sociology, Ahmadu Bello University, Zaria.

Albrecht, T. (2015). Combating Computer Crime. Computer Crime Research Centre.

Ehimen, O. R. & Adekanle, B. (2009). Cybercrime in Nigeria. Business Intelligence Journal 3 (1): 1 – 6

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.

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): 1 – 6

Herselman, M. & Warren, M. (2013). Cyber Crime influencing Businesses in South Africa.

Issues in Information Science and Information Technology 3 (2): 253-266.

Hunda, R. S., Singh, K. & Singh, M. D. (2014). Aspects to Ensure Admissibility of Digital Evidence. Law Journal, Gurn Nanak dev University, Amritsar, 13 (1): 1 – 10

Ibikunle, A. (2005). Investigation of Computer Crime in Information Technology Industry, Unpublished Master‟s Degree Thesis, Ladoke Akintola University of Technology.

Justin P. (2010). Top five computer crimes and how to protect yourself from them. European Journal of Computer Science and Information Technology 6 (1): 11-23

Kirk, G (2008) Cyber Crime and How It Has Affected Society, [Online] Available at http://www.google.com. Retrieved 2nd March, 2016.

Laura, A. (2011). Cyber Crime and National Security: The Role of the Penal and Procedural Law.

Original Article

Longe, O., Ngwa, O., Wada, F, and Mbarika, V. (2009). Criminal Uses of Information & Communication Technologies in Sub-Saharan Africa: Trends, Concerns and Perspectives. Journal of Information Impact 9 (3): 155 - 172.

Matanmi, O., Ogunlere, S., Ayinde, S. & Adekunle, Y. (2013). Impact of Cyber Crimes on Nigerian Economy. The International Journal of Engineering and Science (IJES) 2 (4): 45 – 51.

Mbaskei M. O. (2008). Cybercrimes: Effect on Youth Development. Retrieved 26th March, 2016 from http://www.i-genius.org

McConnell, H. (2000). CyberCrime and Punishment? Archaic Laws Threaten Global Information, [Online] Available: http://www.mcconnellinternational.com/services/cybercrime.htm. Retrieved on 8th April, 2016.

Meke, E. S. (2012). Urbanization and Cyber Crime in Nigeria: Causes and Consequences. European Journal of Computer Science and Information Technology 3 (9): 1-11

Moffitt, T., Pannatia C., Prosenbeck, B., Scott, E. & Siversen, D. (2012). The HRE online Experience-Technology Misuse and Cyber Crime [Online]. Retrieved 15th March 2016 from https//sites.google.com/site/tommoffitt portfolio/the-hre-onlineexperience/technology-misuse-and-cyber-crime.

Moor, J. (1985). What is Computer Ethics? Metaphilosophy 16 (4): 266 - 275.

O‟ Connor, T. (2003). Glee, Elation And Glory As Motives For Cyber Crime, at the Annual Meeting of the Southern Criminal Justice Association, Nashville (March). [Online] Available: http://faculty.ncwc.edu/(toconnor/ gleeelatio nglory.htm. Retrieved 11th March, 2016.

Olumoye, M. Y. (2011). Information and Communication Technology and Data Processing. Lagos, Nigeria: Heralds of Hope Publishers.

Olumoye, M. Y. (2013). Cybercrime and Technology Misuse: Overview, Impacts and Preventive Measures. European Journal of Computer Science and Information Technology 1 (3): 10-20

Parker D. (1983). Fighting Computer Crimes. US: Charles Scribner‟s Sons.

Taylor, P. (2014). Hackers: Crime in the Digital Sublime. Routledge: Wisconsin Publishers, 200

Valacich, J. & Schneider, C. (2010). Information Systems Today-Managing in the Digital World, 4th ed. New Jersey: Pearson.