European Journal of Computer Science and Information Technology

Vol.1, No.3, pp.10-20, December 2013

Published by European Journal of Computer Science and Information Technology

CYBER CRIME AND TECHNOLOGY MISUSE: OVERVIEW, IMPACTS AND PREVENTIVE MEASURES

Mosud Y. Olumoye
Lagos State Polytechnic, SPTSA, Mainland Annex, &
Consultant: ICT, Projects & Safety
Fiatcom Nigeria Limited,
P.O. Box 2090, Ikeja Post Office,
Lagos State, Nigeria.

ABSTRACT: *The harm arising from cybercrime and technology misuse in our society is on the increase and is rapidly claiming attentions both nationally and internationally. The consequence of a single successful cyber attack can have far-reaching implications which may involve huge financial losses, theft of intellectual property, loss of confidence and trust between sellers and customer which eventually affects the economy of a nation. The purpose of this study is to explore the overall view of what cybercrime connotes and the various means through which they manifest in our society. The paper also analyzed the impacts of these crimes and proposed mitigating measures on how it can be alleviated to the barest level if not utterly eradicated from our society.*

KEYWORDS: Computer, Crime, Cyber Crime, Technology Misuse

INTRODUCTION

Society's reliance on computer system has a profound human dimension. In recent years, computers and sharing of information that they facilitate have penetrated nearly every aspect of human life and offers gargantuan benefits to the society. 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 Maitanmi *et al* (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 (Maitanmi *et al*, 2013; Azeez *et al*, 2009).

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 (Mc Connell, 2000).

Herselman *et al* (2005) 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 any one from anywhere in the world (Herselman *et al* 2005; Gordon, 2002). 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 inconvenient 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. The legal system and law enforcement seem not to be keeping pace in tracking down cyber criminals and successfully prosecuting them. 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, T. 2005). Due to this 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.

Concept of Cyber Crime and Technology Misuse

There have been a great deal of debate among experts on what really constitutes a cyber crime or computer related crime. However, there is no universally accepted definition for computer crime; rather functional definitions have been the norm. Cyber crime, which is known to law enforcement as "high technology crime (O'Connor, 2003; Tafoya, 1986; Bequai 1982), and academic researchers as "computer deviance" (O'Connor, 2003; Mercier, 1998), "online crime" or "internet crime" (O'Connor, 2003; Wall, 2001) represents a relatively new field of criminological inquiry that has emerged from the animal justice area of study known as computer crime or computer related crime (O'Conor, 2003; Carter and Katz, 1996; Parker, 1983). Cyber crime may involve criminal activities that are traditional in nature such as theft, forgery and mischief, all of which are generally subject everywhere to criminal sanctions. Cyber crime is ever becoming prevalent in developing countries. In Nigeria for example the cyber criminals are being nick named the "yahoo boys".

According to Valacich *et al* (2010) computer crime is defined as the act of using a computer to commit an illegal act. This definition includes targeting a computer while committing an offense; for example someone gains unauthorized entry to a computer system in order to cause damage to the computer system or to the data it contains. Using a computer to commit an offence in such cases, computer users may steal credit card numbers from Web site or a company's database, skim money from bank accounts, or make an unauthorized electronic fund transfer from financial institutions. And using computers to support a criminal activity, despite the fact that computers are not actually targeted, for example, drug dealers and other

professional criminal may use computers to store records of their illegal transactions (Valacich *et al*, 2010).

A common theme found is this idea that computer crimes are victimless because they only occur in digital form; while there might not be any visible physical damage, there are damages done by computer crimes (Moffit *et al*, 2012). Estimating the incidence, prevalence, cost or some other measures of computer related crime is a very difficult task; cyber crime defies quantification unlike some other criminal act such as theft. This is because some of the most critical crimes perpetrated are never detected, not even by their victims; some are concealed because disclosure of such crime could be embarrassing or commercially inconvenient to victims. Regrettably, a large number of computer crimes (e.g. credit card fraud) go undetected. Research shows us that nine out of ten frauds go unreported (Waugh, 2001). This might be because organizations are apprehensive of reporting computer crimes because it might show susceptibility to future attacks or provide them with unwanted and negative publicity. Also, organizations sweep computer crimes under the carpet for the fear of loosing their customers' base. However, this is unethical for organizations not to inform their customers when they have been held to a computer crime. If customers are unaware of the vulnerability of their personal information then they could be at risk for future attacks and even worse, identify theft. Ethically, we are sending wrong message by not reporting computer crimes no matter the size or damage inflicted (Moffit *el al*, 2012).

Basandra *et al* (2005) pointed out another prevalent concept in cyber crime which is the idea computer criminals preying on the vulnerable. Some criminals argued their actions of breaking into a company's database to prove its vulnerability is a legitimate behavior. They might insist that their actions are not hurting anyone, but in reality they are harming organizations and the public by violating their rights to privacy. However, computer abuse is a little varied from cyber crime. Computer abuse as described by Laudon *et al* (2001) is the commission of acts involving a computer that may not be illegal but are considered unethical.

On the order hand technology misuse is the intentional or unintentional action that harms the technological hardware or software, and the people using the hardware or software. For our purposes, computer crimes fall under the category of harmful actions that are against local, state national and international laws. Technology misuses are often unclear and their legalities blurred as to what is considered against the law and what is not (Moffit *et al*, 2012). Basandra *et al* (2005) identified two common misuse of technology as not using appropriate software or not using the software properly, and inability to keep company and employees data confidentially.

REVIEW OF LITERATURE

Various studies have been conducted on cyber crime. Grabosky (2000) in his paper highlighted that computer related crime poses even greater challenges than conventional ones that have proved to be a very difficult challenge for law enforcement. Since there may be difference between jurisdictions about whether or not the ability in question has occurred at all, whether it is criminal, who has committed it, who should do it and who should adjudicate and punish. Also, there is significant danger that premature regulatory interventions may not only fail to achieve desired effect, may have a negative impact on the development of technology for the benefit of all. Over-regulation or premature regulatory intervention may

run the risk of chilling investment and innovations. And the challenge facing those who would minimize computer related crime is to seek a balance that would allow a tolerable degree of illegality in return for creative exploitation of the technology (Grabosky, 2000).

Mc Connell (2000) pointed out that weak penalties limit deterrence, and global patchwork of laws creates little certainty, that is little consensus exist among countries regarding exactly which crimes need to be legated against. A model approach is needed particularly in the developing world. And that reliance on terrestrial laws is an untested approach especially in the developing countries. In view of this, Mc Connell (2000) suggested three kinds of actions for the weak state of global legal protection against cyber crime; firstly, firm should secure their networked information. Secondly, government should assure that their laws apply to crime crimes. Lastly, firms, government and civil society should work cooperatively to strengthen legal framework of their security.

Herselman *et al* (2003) in their findings pointed out that technology is a double edged sword; good for the good guys and good for the bad guys. This means steps need to be taken to ensure innocent parties are protected regardless of their geographic area. Many countries have taken the initial steps on introductory legislation to protect innocent people. However, until the international nature of cyber crime is matched by the no-so-international nature of law protection can be offered against cross-border crimes.

O'Connor (2003) in his study highlighted that a correct and proper understanding of the motivations for cyber crimes has to go beyond thinking of offenders as enemies, outsiders, super villains, and high tech burglars or robbers. Likewise a proper understanding does not romanticize the offenders as some sort of "hactivist" with an altruistic or revolutionary mindset. There are certainly extremist's motivated by terror and chaos, just as there are undoubtedly disgruntled offenders motivated by revenge and speed. The vast majority of cyber criminals may be simply motivated by glee, elation, and glory, and new directions or outlets for these ordinary quests (or sins) may be a more productive policy avenue than criminalization. Longe *et al* (2007) opined that apart from the issues of piracy and fraudulent scam mails, one major emerging worrisome dimension in the Nigerian cyberspace is pornography in its various guises. The Internet, aided by technology-induced anonymity has popularized the sex business more than any other means of advertisement. With unlimited access to a variety of website, and the impediment of needing to enter a brothel physically removed, immoral gratification is just the click of a mouse away from any intending customer (Longe et al, 2007; Sackson, 1996)

Ibikunle, (2005) in her study pointed out that computing age has brought about opportunities for thieves and crooks. A new degree of complexity has been added to accounting, record keeping, communication and fund transfer. This degree of complexity brings its own set of vulnerabilities which many crooks are all eager to take advantage of. Companies are being blackmailed by cyber criminals who discover vulnerabilities in their networks. Company trade secrets and confidential information are being stolen when security breaches take place. Online banking is accompanied by attendant rise in fraud (Ibikunle, 2005; The News Magazine, 24 Dec, 2004). Longe *et al* (2009) highlighted that cutting-edge technology in computing, telecommunications and electronics has created a digital world in a bewildered pattern of computer networks via telecommunication facilities and thus facilitating the

emergence of the information super highway, otherwise known as the Internet, bringing with it a new networked society and a radical social and cultural metamorphosis.

As electronic commerce and online businesses become a part of today's business world, these types of issues become more important and more dangerous. Hacking and attacks are continually on the increase, and companies are well aware of it. The legal system and laws enforcement seems not to be keeping pace in tracking down cyber criminals and successfully prosecuting them. New technologies to fight many types of attacks are on their ways, but there is need to be proper laws, policies and methods of actually catching the perpetrators and making them to pay for the damage they cause (Ibikunle 2005; Albrecht, 2005).

METHODS USED IN COMMITTING CYBER CRIME

There are numbers of common attacks and methods of committing a cyber crime 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.

- **Malware**: Malware refers to viruses, Trojan worms and other software that gets onto your computer without you being aware it is there. Back in the early part of the century, most of such software's primary aim was for excitement. 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 sinister and that is the reason it makes the list of the top five computer crimes (Anonymous, 2012).

- **Identity Theft**: Identity theft is the appropriation of someone else identity to commit fraud or theft (Sovern, 2004). It makes the list of the top five computer crimes after malware.

- **Cyberstalking**: Cyberstalking is the third on the list of the top five cyber crime after malware. It is essentially using the internet to repeatedly harass (stalk) another person in the traditional sense; the harassment may be sexual in nature or it may have other motivation like anger, outright hostility, cause harm or inflict unwanted advances to another individual. It generally takes place via the internet through the use of chat rooms, message boards, instant massagers, discussion forums, social networks and e-mail. This is as a result of people leaving information about their selves carelessly online; such information makes you vulnerable to cyberstalking.

- **Child Pornography**: This is the fourth of the top five computer crime. However it is catastrophic using the internet to exploit children. What is perhaps horrendous is that people make money doing it.

- **Spam**: These are annoying email messages which are not just irritating but they are big businesses. It is the fifth top five computer crime.

- **Carding**: Stealing credit card information for one's own use or to sell it (Valacich *et al*, 2010).

- **Phishing and Spoofing**: Phishing is described as the criminally fraudulent process of attempting to acquire sensitive information such as usernames; passwords and credit card

details by masquerading as a trustworthy entity in an electronic communication (Moffit *et al*, 2012). Have you ever received an e-mail requesting you to update your bank information, and when you click on the link it takes you to what looks like the current bank's web page? The way it works is you are tricked to go there and update your information on a site that has an ultimate research locator (URL) that is not same as your real bank's URL (Moffitt *el al*, 2012),

- **Hacking and Cracking**: Generally, these refer to the act of gaining unauthorized access to a computer, networks, websites or areas of a system. Hacking is defined as "deliberately unauthorized access to an information system" (Audit commission Report, 2001). Moffitt *el al* (2012) described hacking as the unauthorized access into or interference in a computer system, or any access in order to corrupt, alert, stall or destroy using a computer or other similar information and communication devices, without the knowledge and consent of the owner of the computer or information and communication system including the introduction of computer viruses and the likes resulting in the corruption, destruction, alteration, theft, loss of electronic data messages or electronic document. All these acts are done by hackers. The term hacker originally connotes an undisciplined professional programmer. A hacker is an individual who intends to gain unauthorized access to a computer system. Within the hacking community, the term cracker is typically used to denote a hacker with criminal intent; although in the public press, the term hacker and cracker are used interchangeably (Laudon *et al*, 2010).

- **Eaves Dropping**: This method involves the use of software (sniffers) to monitor packets or wiretapping telecommunication links to read transmitted data. Eaves dropping can go undetected and it is called passive attack. Tools used to intercept communications can be cellular, scanners, radio receivers, microphone receivers, tape recorders, network sniffers and telephone tapping devices (Ibikunle, 2005).

- **Social Engineering**: This is the practice where malicious intruders seeking system access sometimes trick employees into revealing their passwords by pretending to be legitimate members of the company in need of information (Laudon *et al*, 2010). This is also referred to as masquerading.

- **Salami Slicing**: This involves stealing small amounts of money from a large number of financial accounts (Valacich *et al*, 2010). The commonest example of Salami attack is the deduction of a small amount of fund from several accounts with the hope that such an insignificant amount would be unnoticed.

- **Cloning**: This involves the use of scanners to steal wireless transmitter codes for cell phones, then duplicating the phone for illegal use (Valaciah *et al*, 2010).

- **Vishing**: This is also known as voice phishing; instead of asking users to visit a Web site, asking users to call a fake telephone number and "confirm" their accounts information (Valacich *et al*, 2010).

- **Piggybacking or Shoulder Surfing**: This is looking over a person's shoulder while he or she is using an Automated Teller Machine (ATM), cell phone or other devices in order to steal access information (Valacich *et al*, 2010).

- **Daniel of Service (DoS)**: This is any attack that is successful in keeping the legitimate users from the services the computer software provides. This may mean crashing the system or the software.

- **Dumpster Diving**: This type of crime refers to poking through a company's or individual garbage for discarded documents, information and other precious items that could be used to attack against that person or company.

- **Software Privacy**: This involves the use or duplication of an intellectual or creative work of an author without permission or compensation to the author. It is an act of infringement on the ownership rights and if anyone is caught, the person could be sued civilly for damages, be criminally prosecuted or both.

- **Internet Relay Chat (IRC)**: Internet relay chat allows several people from different part of the world to come together and chat with one another like via the internet using chat messages and synchronous forum.

Most of the technologically sophisticated cyber crimes are usually committed using one or more of these methodologies, the result of these attacks are loss of information integrity or authenticity, loss of confidentiality and loss of availability or services associated with the use of the computers, telecommunication equipment or facilities and computer programs.

IMPACT OF CYBER CRIME AND TECHNOLOGY MISUSE

Cyber crime is a huge problem threatening technological advancement and the integrity of the internet as well as our personal lives. 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 cyber crime 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).

Cyber crime has a tremendous impact on the society, although as stated by Kirk (2008) cyber crime 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 cyber crimes is astounding and some of the figures are overwhelming. An example of this is the recognition by the Guinness Book of Word Records is the 1978 bank heist by Stanley Refkin. He used computers to manage a wire transfer to a private account in excess of ten million dollars. That was over thirty years ago and as a whole it is estimated that current cyber crime totals in the billions of dollars (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). 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 *el al*, 2012; Biever, 2005). Also, there is a food-chain effect when society finds out an organization is susceptible to computer crimes. Firstly, the company is made aware of their weaknesses. Customers and companies could potentially lose personal information that could then be sold for a profit. The company then loses credibility and then profits began to fall. Secondly, if the market falls then demand decreases which reduce supply and demand, potentially shutting down a company or sending them into bankruptcy (Muffitt *el al*, 2010).

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 *el al*, 2012). Another impact 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 *et al*, 2009; Cooper *et al*, 2000, Brown and Eisenberg, 1995).

PREVENTIVE MEASURES FOR CYBER CRIMES AND TECHNOLOGY MISUSE

In order to reduce cyber crime and technology misuse to the barest level if not entirely eliminated from our society, the following preventive measures are recommended:

(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.

(ii). Ethical and Moral Standards

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

(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; Mandia *el al*, 2001). 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 Mc Connell (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 (Mc Connell, 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 (Paller *et al*, 2007)

(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.

(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).

CONCLUSION

This study revealed that the society’s dependence on computer systems and the internet which offer great benefits to the society has also presented plenty of opportunities for anti-social and criminal behaviour in untraditional ways. The rapid expansion of large scale computer networks with the ability to access many systems has increased the vulnerabilities of these systems and the opportunity for technical misuse or criminal activity. The consequences of cyber crime are large problems threatening technological advancement, the integrity of the internet, our personal lives, as well as serious economic costs. In view of all these threats being posed by cyber crime it imply steps need to be taken to ensure innocent citizens and organizations are protected regardless of their geographic locations against this menace. It is also very crucial to keep pace in tracking down cyber crime illegality in order to protect the computer system, networks and the data stored on them. Although many developed nations of the world have taken a bold step by introducing various measures on how to combat these threats.

FUTURE RESEARCH

Cyber crime is the fastest growing crime across the globe that no company or nation can tackle alone. There are lots of cyber crime developments that have the highest likelihood of happening, and if they happen would result in huge financial meltdown due to loss of revenue, wasted resources and reduced productivity. These developments include increase in financial cybercrime, espionage, deep infiltration of government agencies and private organizations that stores customers’ data, increase in the numbers of people around the world that would become engaged in cyber crime on full time basis and increase in the sophistication of attacking tools and methods (Paller *et al*, 2007). In view of all these anticipated future challenges, it is very imperative that future research should give a superlative consideration to the next generation internet and the development of cyber security products. Focus should also be more on intimate collaboration between the public and private sector, especially the government agencies, information technology community and academic institutions.

REFERENCES

Albrecht, T. (2005) *Combating Computer Crime*. Computer Crime Research Centre.

Anonymous (2012) *Cybercrime – High Tech Crime*. [Online] Available: www.Sysman.org/ book.htm. Accessed on 8th August, 2005.

Anonymous (2012) *Fighting Cybercrime Making The Future More Secure.* [Online] Available: http://www.bcs.org/content/conWebDoc/8126. Accessed on 25th November, 2013.

Anonymous (2012) *Top Five Computer crimes & How to Protect Yourself From Them*, [Online] Available: http://www.makeuseof.com/tag/top-five-computer-crimeprotect. Accessed on 17th August, 2012.

Audit Commission Report (2001). [Online] Available: http://www.Audit commission.gov .uk/publications/yourbusrisks.html. Accessed on 20th July, 2011.

Herselman, M. and Warren, M. (2003) *Cyber Crime influencing Businesses in South Africa*, Issues in Information Science and Information Technology, 253-266.

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

Kirk, G (2008) *Cyber Crime And How It Has Affected Society,* [Online] Available: http://www.google.com.ng/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&ved=0CFgQFjAE&url=http%3A%2F%2Fwww.iup.edu%2FWorkArea%2FDownloadAsset.aspx%3Fid%3D80833&ei=p0BxUuyHJqO80QXw1oGADQ&usg=AFQjCNHhqenl0xsK-bMLB7x 6b3HpA0YvQg&bvm=bv.55617003,d.d2k Accessed on 28th October, 2013.

Laudon, K. C. and Laudon, J. P. (2010) *Management Information System- Managing the Digital Firm,* 11th ed. New Jersey; Pearson Prentice Hall.

Longe, O. B., Chimeke, S., C., Onifade, O. F.W., Balogun, F. M., Longe, F. A. and Oni, V. U. (2007) *Exposure of Children and Teenagers to Internet Pornograghy in South Western Nigeria: Concerns, Trends & Implications*, Journal of Information Technology Impact, Vol. 7, No. 3, pp. 195-212.

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, Vol. 9, No. 3, pp. 155-172.

Matanmi, O., Ogunlere, S., Ayinde, S. and Adekunle, Y. (2013) *Impact of Cyber Crimes on Nigerian Economy.*

McConnell, (2000) *Cyber Crime…and Punishment? Archaic Laws Threaten Global Information*, [Online] Available: http://www.mcconnellinternational. com/services/cybercrime.htm. Accessed on 8th August, 2005.

Moffitt, T. Pannatia C. Prosenbeck, B. Scott, E and Siversen, D. (2012) *The HRE online Experience- Technology Misuse and Cyber Crime* [Online]. Available: https//sites.google.com/site/tommoffittportfolio/the-hre-online-experience/tech nology-misuse-and-cyber-crime. Accessed on 20th Oct, 2013.

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/gleeelation glory.htm. Accessed on 15th August 2005.

Office of Angel Cruz, Chief Information Security Officer, (2013) *Cyber Crime and How It Affects You,* State of Texas, Vol 7, Issue1. January 2013.

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

Sovern, J. (2004). *Stopping Identity Theft*, The Journal of Consumer Affairs, Madison: Winter 2004. Vol. 38, Issue 2; pp. 233-242.

Thostenson, L. (2013). *Stopping Cyber Crime.*

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

Waugh, D. (2001) *Computer Crime and Ethics*, [Online] Available: http://www. creditcards.com/credit-card-biometric-technology-1273.php. Accessed on 23rd July, 2012.