A Strategic Assessment of Cyber Crime: The Implication and Remedy

By

AKPAN, E. Ebenezer, *Ph.D, FCICN, AP, PPGDCA, PHDCDPM*
Corporate Institute of Research and Computer Science
140 Ikot Ekpene Road
Uyo, Akwa Ibom State

&

Victor Uko EBENEZER
Department of Micro Biology
Faculty of Science
University of Uyo, Akwa Ibom State

Abstract

This study strategically examined the issues of cyber-crime, the implications and the remedies. Cyber-crime is computer oriented and involves computer and network. It evolves from the wrong application or abuse of internet services and this have threatened the country or a person's security and financial health. , the effects of cybercrime are enormous. The resultant effect has turned the world especially when it comes to the issue of financial and business matters. This have to a broader extent deprived most country of the needed Foreign Direct Investment. One of the recommendations was that Open-source intelligence should be gathered by using techniques from social networking sites, web sites and Internet bulletin.

Keywords: Cyber-crime, Cyber space, cyber security.

Introduction

cybercrime is defined as a type of crime committed by criminals who make use of a computer as a tool and the internet as a connection in order to reach a variety of objectives such as illegal downloading of music files and films, piracy, spam mailing and the likes. Cyber-crime evolves from the wrong application or abuse of internet services. The computer maybe it`s target or used in the commission of the crime. Cybercrimes can be defined has: "Offences that are committed against individuals or groups of individuals with a criminal intension to harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet. It also used to describe any criminal activity that involves the computer or the internet network (Okeshola, 2013). The term cyber-crime is also used for crimes such as fraud, theft, blackmail, forgery, and embezzlement, in which computers or networks are used, (Maitanmi, 2013). The concept of cybercrime is historical. It was discovered that the first published report of cybercrime occurred on the mainframe computer in the 1960s (Maitanmi, 2013). Since these computers were not connected to the internet or with other computers, the crime was committed by the employers (insider) in the company, hence it was referred to as computer crime rather than cybercrime.

Cybercrime has threatened people or the nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those

surrounding hacking, copyright infringement, unwarranted mass surveillance, extortion, child pornography, and child grooming. A report (sponsored by McAfee), published in 2014, estimated that the annual damage to the global economy was $445 billion and that close to $600 billion, nearly one percent of GPD is lost to cyber-crime each year. Presently, cybercrimes are performed by people of all ages ranging from young to old, but in most instances the young. However, a report reveals that 48.6% were females, 46% were males and the remaining 5.5% were anonymous. The method or instruments of the attacks include phishing and spamming with 4.4 %, Phone hack with 16.3%, Social network attack with 13.2%, Internet fraud with 9.8%, text message with 4.2%, (Scam Watch).

A research by (Olayemi, 2014) suggests that billions of naira were lost to cyber theft, the majority of which was caused by either software vulnerability, unawareness, carelessness or direct attack on assets with the intention to cause implicit damage. He added that a report shows that "The general distribution of cyber-attacks is that 50% are activism, 40% are cybercrimes, 7% are cyber espionage and 8% are cyber warfare" (Odeyemi, 2013).

Statement of the problem

In recent times, our society is increasingly relying on the internet and other information technology tools to engage in personal communication and conduct business activities among other several benefits. While these developments allow for enormous gain in productivity, efficiency and communication they also create a loophole which may totally destroy an organization. The crime usually requires a hectic task to trace. These crimes usually affect the victim directly or indirectly such as fraud, scam, and theft of information.

It has been discovered that youths are the most users of the internet, thus, they see the internet as an easy means of earning livelihood and quick money. This largely predisposes the youth to all nook and cranny of the cybercrime and other related offences. This category of youth is popularly called in Nigeria as "yahoo boys". Lack of strong Cyber Crime Laws have also encourages the perpetrators to commit more crime knowing that they can always go uncaught. The contribution of the internet to the development of the globe has had a positive impact on various sectors of the country. However, these sectors such as the banking, ecommerce and educational sector battles with the effect of cybercrimes. More cybercrimes are arising at an alarming rate with each subsequent crime more advanced than its predecessor. There is need for our government to come up with stronger laws and be able to enforce such laws so that criminals will not go unpunished.

Objective of the study

The main objective of this study is to examine the effect of cyber-crime and the needed remedy. Specifically the following objectives have been drawn.

1. To examine the effect of cyber-crime.
2. To determine the needed remedy to the problems of cyber-crime.

Literature Review

Cyber Space

In recent times, revolutionalisation of modern information and communication technology system gave birth to cyberspace, a horizon that provides unlimited opportunities through which communication takes, thus, creating possibilities and chances for expansion on the existing

internet, networking, and other digital communication systems. It has removed the barriers within and among nations, as well as opened a gate for contested spaces, making it possible for the proliferation of information and communication through the utilization of computer, internet and other related communication systems. It also provides a window view to a successful business, administrative and diplomatic opportunities, as well as the removal of most barriers among the international community.

Implication of Cyber Crime

Cybercrime has drastic effects on nations such as financial loss. Cybercriminals are likened to terrorists due to the fact that their acts force impromptu expenses on the citizens and society at large; loss of reputation/ image defamation-organizations that have been swindled or reported to being attacked by the activities of cybercriminals face the loss of customers' confidence in them; reduced productivity-which is caused by more fixation on forestalling cybercrime thereby leading to unprofitability, it also slows production time and adds to overhead cost, cybercrime leads to vulnerability of their ICT systems and networks and time wastage (Ibikunle & Eweniyi, 2013).

Cybercrimes have surpassed traditional violations and now have frightening implications to the national security of all countries in the international system, even to technologically advanced countries like the United States (Ibikunle & Eweniyi, 2013).

There is additionally a need to build up an information society that regards values, rights and freedoms and guarantees same access to data, even as mixing up the foundation of bona fide knowledge can set up confidence in the utilization of ICTs (Ibikunle & Eweniyi, 2013; United Nations Economic Commission for Africa, 2014cited in Oforji, 2017). This include the areas of education, governance, politics, business, agriculture and the likes, the use of the Internet is involved, basically for easy communication and faster delivery of services. This aligns with the position of Ibikunle and Eweniyi who submit that cyber space has transformed the ways we communicate, travel, power our homes, run our economy, and obtain government services. Meanwhile, the involvement of Internet in various operations and services in the country by both public and private sectors require protection and security, due to emergence of cybercrimes.

In addition, there are also emerging cyber tricks. When a proper check on the systems in done, the administrators can be able to block any future occurrence of such attack. Sometimes if lucky, the attacker can even be traced by law enforcement agencies just as it happened in the famous EFCC cases of Elekwe and Yekini Labaika who defrauded a Brazilian Bank and forced it to be closed completely. A recent prediction by the Central Bank Governor Mr. Godwin in while speaking at the Quarterly Meeting of the Chief Audit Executives of Banks with the motto "Changing Business Environment" says "Losses due to cybercrimes across all sectors have been estimated globally to hover between $400 to $550 billion in 2015". He added that the figure could increase to about $2 trillion dollars by the end of 2019 (Okafor, 2017).

Nevertheless, it is equally important for us to understand and acknowledge the undoubted fact that the problem of cyber fraud has now become global in both scope and impact. Hence it is a global issue that requires helping hands from across the globe coming together to fight it.

Trojans or Trojan horses are unauthorized malicious programs that usually pretend to be authorized and on the basis of which they target systems (Ibikunle & Eweniyi, 2013). Some of the forms of Trojans identified by experts are hand on theft Trojan, remote access Trojan, data

sending Trojan, destructive Trojan, denial of service Trojan and security disabler Trojan. In a nutshell, malware are programmable codes or components designed purposely to damage, destroy, deny access and or cause the target system to work based on how the attacker wants (Mattord, 2012). It is in the light of this that Fortinash and Holoday-Worret (2012) describe cyber murder as internet homicide which, according to them, refers to a kind of killing aided by the internet which facilitates the online meeting of the victim and the perpetrator. Many reports have revealed that several murders were committed as a result of medical equipment being hacked (ICIT), (Filkins, 2014). Cyber-criminal are also engaged to murdering by remotely altering his prescribed drugs by hacking the hospital computer system.

It is mentioned that most of the victims are of cyber-crime are banks, computer companies like Microsoft, Online Sellers and Email service providers like Yahoo! and Google (Razzaq, et.al. 2013).

Remedy of Cyber Crime

Cybercrime is a systematic and intentional use of technical criminal skills that involves information and communication knowledge to illegally hack and have access to scribed or coded information by interception of data through unauthorized damaging, manipulation or distortion, diversion, hijacking, retrieving, deletion, deterioration, alteration or suppression, inputting, transmitting, deleting, forgery or theft of computer data or information and transactions. Cyber-security should be set up which is the body of rules put in place for the protection of cyber space. Ensuring cyber-security requires coordinated efforts from both the citizens of the country and the country's information system. . Code obfuscation is the deliberate act of creating the source codes which are difficult for human beings to understand (Michael (2012), this will help prevent attackers, for there will not be able to find the source code and thereby cannot login to the site. Also if the cyber-crime bill which is "A Bill for an Act for the Prohibition, Prevention, Detection, Response, Investigation and Prosecution of Cyber Crimes and for Other Related Matters, " is well enforced, it will help reduce cybercrime. The bill was set up to provide a legal framework for the implementation and evaluation of response and preventive measures in the fight against Cyber Crime as well as other related frauds in line with international best practices. It was also set up to provide a legal framework for the prohibition and punishment of electronic fraud and cybercrime whilst promoting e-government services, electronic communications and transactions between public and private bodies as well as institutions and individuals. The bill seeks to criminalize certain acts and omissions in line with regional and international best practices and provide procedural guidelines for the investigation of such offences. The legislation also defined the liability of service providers and ensures that the national interest is not compromised by the use of electronic communications. During the bill's public hearing, stakeholders and the general public made some important contributions to the bill which specifically seeks to secure computer equipment against unauthorized access and modification, as well as against misuse in the following areas: (1) Unauthorized access or modification of computer. (2) Unauthorized access with intent to commit or facilitate commission of further offences. (3) Unauthorized access to computer or misuse of electronic devices.

Public awareness should also be made by the government to educate the general public especially the internet users on the criminality of cyber-attack. An effective cyber security environment is needed and must ensure legal compliance, technical competence and other required organizational measures, such as, capacity building and cooperation for it to be effective. It is when this is done that proper growth can be achieved, and citizens' rights not

threatened.

Conclusion

In conclusion, the effects of cybercrime are enormous. The resultant effect has turned the country against the international community especially when it comes to the issue of financial and business matters. This to a broader extent has deprived the country of the needed Foreign Direct Investment required to propel the economy the level of advancement. An effective cyber security environment is needed and must ensure legal compliance, technical competence and other required organizational measures, such as, capacity building and cooperation for it to be effective. It is only when this is done that proper growth can be achieved, and citizens' rights not threatened.

Recommendation

1. Training courses on countering cybercrime should be developed and made available by the government to help educates its citizens about the threat of cyber-crime.

2. Open-source intelligence should also be gathered and made available using techniques from social networking sites web sites and Internet bulletin.

3. The users of the internet should install anti-virus software on their computers to help detect treat or theft of file from another user.

REFERENCES

Filkins, B (2014), *Health Care Cyber threat Report*, compliance nightmare horizon. Bethesda, *MD*.

Fortinash, R. and Holoday-Worret, E. (2012) Scholarly articles. *The Information on Security Legislations*.

Ibikunle, Y. & Eweniyi, T. (2013), *Approach to cyber security issues in the globe*: Challenges and solution.

ICIT (2016), Hacking Health care IT in 2016. *International Journal of Advanced Research in Computer and Communication Engineering*, 5(3)

K. Michael (2012). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*, 3(1).

Maitanmi, W. (2013), Impact of Cyber Crimes on the worlds Economy.

Mattord H. J. (2012), *Principles of Information Security Fourth Edition*, 4th Edicat. Cengage Learning.

Odeyemi D. D. (2013), Cybercrime Event. ARPN *Journal of Science and Technology*, vol. VOL. 2(7), 626 – 631

Oforji J. C. (2017) cyber security challenge' in recent times. *The International Journal of Engineering and Science (IJES*), Vol. 2 (4), 45–51.

Okafor P, (2017) Nigeria: Global Cybercrime Loss to Hit U.S.$1.5 Trillion By 2019, *Vanguard Newspaper*, Lagos, Nigeria,

Okeshola I. (2013). *The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State*, Nigeria. Term paper, University of Calabar.

Olayemi O. J. 2014, A socio-technological analysis of cybercrime and cyber security, *International Journal of Sociology and Anthropology* 6(3), pp. 116–125.

Razzaq, A. Hur, H. F. Ahmad, and M. Masood (2013), "Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications,"*2013 IEEE Elev. Int. Symp. Auto. Decentralized Syst.*, pp. 1–6.