THE STATUS OF CYBER CRIMES IN ZAMBIA

BY

SOMBO CHINYAMA

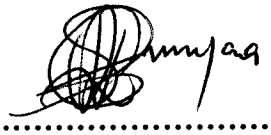
A paper presented in partial fulfillment of the requirements for the award of Bachelor of Laws degree of the University of Zambia.

April, 2011

DECLARATION

I, **Sombo Chinyama**, Computer Number **27134636** do hereby declare that the contents of this Dissertation are based on my own findings. I further declare that the information used herein that is not my own I have endeavoured to acknowledge.

I, therefore declare that all errors and other shortcomings contained herein are my own.



.....

SIGNATURE

14th April, 2011

.....

DATE

THE UNIVERSITY OF ZAMBIA

SCHOOL OF LAW

I recommend that the obligatory essay prepared under my supervision by

SOMBO CHINYAMA

Entitled

THE STATUS OF CYBER CRIMES IN ZAMBIA

Be accepted for examination. I have checked it carefully and I am satisfied that it fulfills the requirements relating to format as laid down in the regulations governing obligatory essays.

Supervisor:..... Date:.....

JUDGE KABASO CHANDA (Rtd)

ABSTRACT

Cybercrime cut across territorial borders, creating a new realm of illegal human activity and undermining the feasibility and legitimacy of applying laws based on geographic boundaries. Nations are finding cybercrime deeply threatening. It is subjecting States to unprecedented challenges with regard to their efficacy, sovereignty and functions. The past several decades have brought a vast increase in the availability of electronic resources. Technologies such as cellular phones, home computers, the internet and websites have added another dimension to crime. That dimension involves increased methods at criminals' disposal to commit certain crimes along with increased locations in which crimes can occur. With this increased availability of technology has come this form of criminal activity that takes advantage of electronic resources. Currently, these new forms of crime are burgeoning and pose a new and lasting challenge to law enforcement agencies at all levels on how to prevent, investigate, and prosecute these crimes. Computer crime poses a daunting task for law enforcement agencies because they are highly technical crimes.

Accordingly, this paper seeks to address and analyse the following issues: Firstly, it raises awareness with regard to the rise of crime in cyberspace. Secondly, the essay examines the nature of the crime, what cybercrime is, the types of cybercrimes, how the crimes and committed some of the reasons why criminals engage in these crimes. Thirdly the essay looks at the prevalence or the status of cybercrimes in Zambia and the response on measures being taken by the relevant stakeholders. Finally, the paper would conclude by discussing the steps that should be taken in the battle against these crimes.

ACKNOWLEDGEMENTS

Firstly, I thank the Lord God Almighty for being my pillar in everything I do. He has paved ways where things were extremely difficult and preserved my life in order for me to be able to accomplish this work and my studies generally. Thank you Lord for being a God to me, I will live to praise your Holy name. Amen!

Secondly, heartfelt thanks go to my Supervisor, Judge Kabaso Chanda, for his supervision and guidance without which, it would not have been possible to put up this scholarly work.

The author is also indebted to the scholastic prowess prevailing in the School of Law at the University of Zambia. The invaluable contributions of the learned women and men lecturing in the School have molded me into a Lawyer. Their determination will certainly for a long time to come linger in my mind.

Further acknowledgements go to the following people for their invaluable assistance.

1. Mr. Rodgers Phiri - The Systems Development Manager at the Centre for Information and Communication Technologies at the University of Zambia
2. Mr. Mukuka Chileshe - The Supervisor for Financial and Computer Fraud Investigations at the Police Headquarters - Lusaka
3. Mr. Emmanuel Chimuka - IT Manager at ZSIC and also the Chairman for Midlands in the Computer Society of Zambia
4. Mr. Garry Mukelabai - ICT Manager at Zambia Information Communication Technology Authority (ZICTA)
5. Mr. Munukayumbwa Lubasi - The Senior Principal Officer for IT at the Ministry of Communications and Transport
6. Mr. Musona - The Registrar of the Judiciary at the Supreme Court of Zambia
7. Mr. Kasonde - Senior Clerk of Court at the Magistrate Courts Complex
8. Mr. Lipimile Kapelwa - Assurance Manager at Standard Chartered Bank

9. Mr. Kenny Bobo - Information Technology Manager - Zambia National Commercial (ZANACO) Bank Headquarters, Lusaka

10. Mr. Musonda Kapaya - Chief Information Security Officer - ZANACO

11. Mr. Shepherd Hampako

12. Mrs. Florence C. Lubasi

13. Lastly though not the least, I thank all those who could in one way or the other contributed to the successful completion of this work. God bless you all!

DEDICATION

To my dear husband, Collins, for the enormous support in all aspects of my life and my precious children Wana, Pezo and Chisambo who had to forego so much, financially and quality time with me in order to enable me realize my dream and to my late daddy (Joseph Mutondo Chinyama) who imparted the value of education in me as well as my mother (Alice Muke) who went out of her way to make my early school life comfortable. God bless you all for being there for me!

ACRONYMS AND DEFINITIONS

IT	-	Information Technology
ICT	-	Information Communication Technology
ZP	-	Zambia Police
CSZ	-	Computer Society of Zambia
ISP	-	Internet Service Provider
ZICTA	-	Zambia Information and Communication Technology Authority
ATM	-	Automated Teller Machine
Email	-	Electronic Mail

Computer	-	An electronic machine that can store, organize and find information, do calculations and control other machines.
Cyber	-	Connected with electronic communication networks, especially the Internet
Cyberspace	-	The imaginary place where electronic messages, etc. exist while they are being sent between computers.
Crime	-	An act, default that involves breaking the law
Network	-	A number of computers and other devices that are connected together so that equipment and information can be shared.

TABLE OF STATUTES

1. The Electronic Communications and Transactions Act No. 21 of 2009

TABLE OF CASES

1. The People v. Charlie Tommy and 5 Others (CRMP-18-2010)
2. The People v. Chibuye Mwanje 2SP/C/132/09
3. The People v. Dominic Mukuka Tresha, Humphrey Chewe and Nephas Kango (2SP/C/01/2010)
4. The People v. Oscar Chizanda (SSP-20-2007)
5. The People v. Yusuf Pando and Bengula Beyani (2SP. 13.2004)

TAB LE OF CONTENTS

Content **Page**

CHAPTER ONE

1.0 THE RISE OF CRIME IN CYBERSPACE

Introduction

The term "cyberspace" was coined by the science fiction author William Gibson in his 1984 novel *Neuromancer*, to describe the environment within which computer hackers operate.[1] The activity of hacking securing unauthorized access to the contents of computer systems is couched in very physical terms.[2] The image is of the hacker overcoming physical security barriers to penetrate into the heart of computer systems and make changes to the physical structure thereby modifying the operation of the system. When departing, the hacker might even remove and take away elements of the system.

Cyberspace radically undermines the relationship between legally significant online phenomena and physical location.[3] The rise of the global computer network is destroying the link between geographical location and the power of local governments to assert control over online behaviour, the legitimacy of the efforts of a local sovereign to enforce rules and the ability of physical location to give notice of which sets of rules apply.[4] Faced with their inability to control the flow of electrons across physical borders[5] some legislators strive to inject their boundaries into electronic mediums through filtering mechanisms and the establishment of electronic barriers.[6]

---

[1] In fact, the term cyberspace literally means 'navigable space' and is derived from the Greek word *kyber* (to navigate). In William Gibson's 1984 novel, the original source of the term, cyberspace refers to, a navigable, digital space of networked computers accessible from computer consoles, a visual, colourful, electronic, Cartesian data space known as 'The Matrix' where companies and individuals interact with, and trade in, information. Since the publication of this novel, the term cyberspace has been reappropriated, adapted and used in a variety of ways, by many different constituencies, all of which refer in some way to emerging computer-mediated communication and virtual reality technologies. Here, we refocus the definition back to the envisaged by Gibson, so that cyberspace refers to the *conceptual space* within ICTs, rather than the technology itself. W. GIBSON, *Neuromancer* (New York, Grafton), (1984); M. DODGE, Mapping Cyberspace (N.Y, Routeldge), (2001) p. 1.

[2] C. REED, *Computer Law* (U.K, John Angel), (2004) p. 242.

[3] Mohamed CHAWKI; A Critical Look at the Regulation of Cybercrime: A Comparative Analysis with Suggestions for Legal Policy; LL.B (1998), pg 6

[4] D. Johnson and D. Post, Law and Borders: The Rise of Law in Cyberspace(Stanford, Stanford Law Review), (1996) No. 1378.

[5] Mefford, Lex Informatica: Foundations of the Law on the Internet (IJGLS), [1997], 5(1) p.212.

[6] Karen Kaplan, Germany Forces Online Service to Censor Internet, L.A. Times, (Dec. 29, 1995), at A1

The past several decades have brought a vast increase in the availability of electronic resources and activities. Technologies such as cellular phones, pagers, home computers and internet, websites have added another dimension to crime. That dimension involves increased methods at criminals' disposal to commit certain crimes along with increased locations in which crimes can occur. For example, property crimes no longer have to involve face-to-face contact between the criminal and the victim. In the past, property crimes usually involved a criminal breaking into a victim's house or grabbing a purse from a person on the street. Today, criminals can commit property crimes from the comfort of their own homes against people who live on the other side of the world through the use of computers.

1.1 STATEMENT OF THE PROBLEM

As our lives have become inexorably intertwined with the computer and other digital devices, Zambians have been slow to understand the magnitude of change both for the better and for worse. We have not scratched the surface of understanding the impact of technology on deviant behavior both criminal and non-criminal. We do know that computers, and the information in them, have expanded the ability of criminals to perpetrate traditional crimes while posing huge hurdles to the criminal justice system. It is important to look at how the challenge is distinct from other law enforcement challenges, to recognize the macro issues involved, and to ensure that there is appropriate focus to addressing the long-term problems as well as the immediate needs of the enforcement communities. Successful response to these challenges requires new paradigms.[7]

As the Internet has become a needed tool at home and in businesses it has also become a tool and target for crime. The anonymity of the internet allows for all sorts of illegal activity to take place without many repercussions. Until recently, law enforcement has seen cyber-crime as insignificant and not worth their time. Due to companies' reliance on the internet and their

[7] **Dick Johnston:** Abstracts for Cyber Crime Summit: A Unique Challenge Requiring An Innovative Response; http://www.infolizer.com/3crim5e-r5es5e1ar3ci8a1or7g/Abstracts-for-cyber-crime-summit.html; visited: 30/08/2010

computer networks the losses sustained are often large and potentially catastrophic. Technology has always provided new ways of solving old problems as well as distributing information. The internet has made all types of information readily available. This wealth of information has opened up a whole new world of problems. These problems deal with the security of computer networks. As the general public has gotten more technologically advanced so too has the criminal. It is important for current and future members of the business world to understand these crimes, the motivations for such crimes and what can be done to find and stop such criminals before Zambian businesses collapse altogether.

1.2 RATIONALE, JUSTIFICATION OR SIGNIFICANCE OF THE STUDY

As the world edges itself into the cyber-information age without much of a commotion,[8] governments the world over eye this as technologically rewarding and are eagerly intent in pushing for internationally acclaimed Information Communication Technology (ICT) literate nations that are completely aware of the importance of ICT toward sustainable social and economic development. As much as the world approves of, globalization and quicksand-speed technological advancement have placed knowledge on the brazen frontlines of the competitive world economy. In highlight of that, Zambia recognizes the importance of effectively utilizing ICT in education, tourism, business and many other areas to cushion the growing demand for a highly-skilled work force that excels in various aspects and most importantly, versatile in the sense of being able to adapt to whatever environment is subjected on them as a result of the rapidly expanding economy.

ICT has also been shown to be positively, if not proportionally, related to a country's economic development and opportunities. The Zambian private sector is now heavily relying on ICTs to deliver all their services country-wide. Almost all the companies in Zambia have computers in their offices which are used for their operations. Therefore, the survival of these companies is dependent on the safety of these computers.

[8] **Ling Wai Chyuan**; The importance of ICT for development, 2008 (www.unapcict.org/ecohub/resources/browse.../asean.../ict4d.../file) visited30/08/2010

Mobile technologies have also mushroomed at a faster rate in the country and are now being used as a channel for commerce and industry. Business competitions, banking, education are all being carried out through the mobile phones. Cyber criminals are now launching attacks through mobile phones by tapping secret conversations between people. Secret conversations among business partners, government officials and even private individuals, have been heard by people who should not hear them.

The internet is increasingly used as a tool and medium by transnational organised crime.[9] Through this scheme, a great number of Zambians have lost their hard earned money. Sometimes, these cyber criminals would hack into someone's email account and then gain access to his clients. With this access, these criminals then impersonate the account owner and send messages to his friends and relatives claiming that he is stranded in some part of the world and he needs help, which the panicking relatives and friend send without realizing that they have actually been crooked.

The flexibility of Automated Teller Machines (ATMs) Cards in depositing and withdrawing money is a tremendous revolution which has wooed a number of Zambians. These ATM cards have made business easy to carry out and execute because people no longer have to carry bunches of money when going for orders. In July 2010, there was a severe cyber crime in Zambia involving ATM Cards where a number of bank customers lost their money when their cards were replicated and used by criminals to withdraw money.[10] While the major industrialized countries change their cyber legislations as technology changes, Zambia like many other developing countries has remained static which makes the country a prime target for cybercrimes and presents the cyber criminal a safe haven to operate in, hence the need to educate people about these crimes. Never before has the need to fight cyber crimes been higher than now.

---

[9] In fact, the involvement of organised crime groups in the field of computer fraud was illustrated when a Russian group attacked one of the best known US banks in New York via data networks in 1994. Operating from St. Petersburg, the group succeeded in causing the American bank to transfer over US$ 10m to foreign accounts. Monitoring and following the "money trail" of the manipulations, some of the perpetrators finally could be arrested. The responsible security officer of the bank reported that the arrested perpetrators possessed false Greek and Israeli passports which were forged in a quality which could be produced in Russia only by members of the former Russian secret service KGB. *See* M. LYMAN and G. POTTER, *Organized Crime* (New Jersey, Prenhall); U. SIEBER, *Legal Aspects of Computer Related Crime* (European Commission) [1998] p. 25.

[10] Bankers' Association of Zambia Chairman Saviour Chibiya; Zambia hit by alleged debit card fraud: Post Newspaper of Thursday, 29 July 2010.

All these beneficial services are tremendously under severe threat due to increased levels of cyber crimes. Due to the nature of these crimes, sometimes they go unnoticed for long periods of time. These cyber crimes are now sitting on the successes that has been scored by the Private Sector. Most companies in Zambia are becoming very skeptical on whether to continue using computers and the internet for the provision of their services or not as Cyber criminals have been terrorizing companies, but these crimes have not been sufficiently reported for fear of losing out on business and scaring away customers.

1.3 OBJECTIVES OF THE STUDY

The study aims to achieve the following:

1.3.1 Creating awareness among Zambians on the prevalence of these crimes in the Nation

With the information highway having entered our offices and homes, we are all at increasing risk of being affected by cybercrime. Everything about our lives is in some manner affected by computers. Under the circumstances it is high time we sat up and took notice of the events shaping our destinies on the information highway. Cybercrime is everyone's problem, and it is time we did something to protect ourselves. Information is the best form of protection.

1.3.2 To show that fighting cyber crimes cannot be done within the confines of one country since these crimes can be committed by a person from another country

Cybercrimes cut across territorial borders, creating a new realm of illegal human activity and undermining the feasibility and legitimacy of applying laws based on geographic boundaries.[11] Territorially based law making and law enforcing authorities find cybercrime deeply threatening.

[11] Mefford, Lex Informatica: Foundations of the Law on the Internet (p. 212)

1.3.3 To educate the masses on the various preventive measures that can be undertaken in order to minimize or to protect themselves from cyber crimes

Preventing computer crime is much easier than detecting it once it has been committed. There are some basic steps that any manager or network administrator can take in order to prevent the commission of cyber crimes. None of these are full proof, but they help reduce the chances of an organization being the victim of cyber criminals.

1.3.4 To equip the police, the lawyer and the justice system as a whole with investigative skills necessary to identify perpetrators of cyber crimes

There is need to educate and train everyone who will be involved in preventing, detecting, reporting, or prosecuting cybercrime. Prosecuting attorneys need training to understand the meanings of various types of digital evidence and how to best present them at trial. Legislators also need to understand the laws they propose and vote on.

1.3.5 To give the status of cyber crimes in Zambia and what is being done to combat or arrest the situation

It is a fact that Zambia has not been spared by this new form of crime. The aim of this essay is to try and find out the extent to which Zambia has been hit and what if any is being done in the pursuit to answer the nagging question, is the current legal framework work able to handle cyber crimes?

1.4 UTILITY OF THE STUDY

Cybercrime is a persisting international evil that transcends national boundaries in a manner that renders this form of organized crime a global concern. Cybercrime may take several forms including online fraud, theft and cyberterrorism. It has been seen that amongst the major reasons that facilitate the perpetration of this crime is the globalisation of technology and the revolutionary advancement of ICTs. Broadband, wireless technologies, mobile computing and remote access, Internet applications and services, software and file transfer protocols are

amongst the tools utilized by cybercriminals to commit their crime. The increasing proliferation in usage of technology assisted criminal activity and cybercrime merits further attention from the global community by enacting the necessary legislative provisions and implementing effective technological and enforcement tools that reduce ICT-facilitated criminal activities.[12] Hence, this kind of study is timely bearing in mind the outbreak of these crimes in Zambia in the recent past.

1.5 SCOPE OF THE RESEARCH

The aim of this essay is to review the status of cyber crimes in Zambia. The reason being to raise awareness among the populace on these crimes which apparently are a new phenomenon in our country bearing in mind that knowing how much crime is committed might help the Government, private sector and all stake holders to decide on how much to spend on security.

1.6 METHODOLOGY

The essay which is a qualitative research would be mainly done by desk research. Relevant published and unpublished work will be consulted. Case law as well as other relevant pieces of legislation will be consulted. The internet as a source of data will be greatly utilized. Visitations to relevant institutions like Ministry of Communications and Transport, Financial institutions, Police, Judiciary (Courts) will be conducted and direct interviews with personnel concerned will be held. The research questions will include; what is cybercrime? Has your institution experience cybercrime? What measures have you put in place to mitigate future risks? Are there any recorded cases on cybercrimes?

1.7 ESSAY DESIGN

The chapter outline of the essay would be as follows. The introductory chapter is named, 'The Rise of Crime in Cyberspace' and it contains the statement of the problem which is aimed at explaining the nature of the assignment to be undertaken because as the internet has become a

[12] Mefford, Lex Informatica: Foundations of the Law on the Internet, p. 212

needed tool at home and in businesses it has also become a tool and target for crime and so it has presented a problem worthy investigating. The chapter also contains a section on the rationale, justification or significance to spell out the importance of the study under review. There are also a number of objectives set out to be met under the study for example one of the objectives is to educate and train everyone who will be involved in preventing, detecting, reporting, or prosecuting cybercrime. The chapter also has sections on utility, scope and methodology of the study to be taken.

Chapter two is named, 'The Nature of the Crime' and it houses sections on defining the crime, elaborates on some of the types of cybercrimes, it also shades light on the concept of cybercrimes in a little more detail and shows how the crimes are committed and reasons why people commit cybercrimes.

'The Prevalence of cybercrimes in Zambia' is dealt with in chapter three of the essay. Under this chapter the paper looks at the case study in regard to thefts on Automated Teller Machines (ATMs), crimes being perpetuated through phones, especially cellphones. There is also a section on electronic mails (Emails) which shows the crimes committed through the internet and finally there is a section on computer systems and applications.

Chapter four is designed to look at the 'Measures that are being Contemplated' by the various stakeholders, which includes the government as the major stakeholder, the Financial Sector, the Zambian Police and the ICT sector to try and combat the rise of these crimes. And finally, chapter five is the recommendations/conclusion chapter of the whole essay.

Having clearly introduced the topic and elaborated on the need and justification for undertaking the research, the author now proceeds to show the nature of cybercrimes in more detail and give an indication of the status of cyber crimes in Zambia.

CHAPTER TWO

2.0 THE NATURE OF THE CRIME

Threats posed to organizations by cyber crimes have increased faster than potential victims or cyber security professionals can cope with them, thus placing targeted organizations at significant risk. Today's cyber criminals are increasingly adept at gaining undetected access and maintaining a persistent, low-profile, long-term presence in information technology environments. Many are failing to recognize cyber crimes in their information technology environments and misallocating limited resources to lesser threats. For example, many organizations focus heavily on foiling hackers and blocking pornography while potential and actual cyber crimes may be going undetected and unaddressed. This has generated significant risk exposure, including exposure to financial losses, regulatory issues, data breach liabilities, damage to brand, and loss of client and public confidence.[13] Cyber crimes are much more dangerous because they can be going on over and over but without detection at all.[14]

Cyber criminals can actually be committing criminal activities while chatting with the owners of the organization over a cup of tea. This happens when the owners of the organization do not posses any significant skills in cyber security. They may be seeing as if someone is just doing some typing on the computer and yet he is sabotaging their systems. The other challenge for cyber crimes is that they can be committed virtually from any point in the world.[15] A cyber criminal can, for example sit on his computer say in Venezuella and be able to commit a crime here in Zambia. The challenges of detecting the source of these crimes are considerably high thus allowing most criminal activities to go on un reported.

---

[13] Sweetmir; Cyber Crime: The Risk, Danger and Trends: April, 2010 (http://hubpages.com/hub/Cyber-Crime-The-Risk-Danger-and-Trends) visited 30/08/2010

[14] Tom Olzak, The five phases of a successful network penetration: December, 2008, http://www.techrepublic.com/blog/security/the-five-phases-of-a-successful-network-penetration/701, visited 30/08/2010

[15] Howard Haines; Cybercrime Law Separating Myth from Reality: April, 2010 (http://www.articlesbase.com/k-12-education-articles/cyber-crime-law-separating-myth-from-reality-711755.html) visited 30/08/2010

Production of evidence in a cybercrime case is extremely difficult as it requires highly sophisticated cyber tools most of which do not exist in most countries among law enforcement agencies. It is a known fact that most lawyers, judges and police officers are not well equipped on cybercrimes and thus fail to adequately prosecute criminals in court. These factors are significantly leading to a rise in cyber crimes in Zambia and the world over. Another challenge in prosecuting cybercrimes relates to the ever changing and evolving technologies. As technology changes so also are the tools for cyber criminals. This makes law enforcement officers fail to fully identify and fight these crimes because while they are still struggling to learn one tool to detect cyber crimes, the criminals change the tool and use another one making eradication of cyber crimes extremely hard to achieve. The only way is for significant awareness raised among individuals, organizations and government while severely punishing the few cyber criminals who are caught.

2.1 DEFINING CYBER CRIME

What is cybercrime? Law enforcement experts and legal commentators are divided on this point. Some experts believe that computer crime is nothing more than ordinary crime committed by high-tech computers and that current criminal laws on the books should be applied to the various laws broken, such as trespass, larceny, and conspiracy. Others view cyber-crime as a new category of crime requiring a comprehensive new legal framework to address the unique nature of the emerging technologies and the unique set of challenges that traditional crimes do not deal with; such as jurisdiction, international cooperation[16] intent, and the difficulty of identifying the perpetrator.

Computer crime or cybercrime refers to any crime that involves a computer and a network,[17] where the computers may or may not have played an instrumental part in the commission of a crime[18] while net crime refers more precisely, to criminal exploitation of the Internet.[19] Issues

[16] Eric. J. Sinrod and William P. Reilly; Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws, Computer and High Technology Law Journal, Vol.16 (2000)
[17] Rassolov, I. Law and Internet – M., 2003. – P.257 (http://www.crime-research.org/library/Nomokonov.html) visited 31/08/2010
[18] Moore, R.; "Cybercrime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing (2005)
[19] Mann and Sutton; Netcrime: More change in the Organization of Thieving. British Journal of Criminology; 38: 201-229, (1998) http://bjc.oxfordjournals.org/content/38/2/201.short visited 07/09/2010

surrounding this type of crime have become high profile, particularly those surrounding hacking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise. On the global level, both governments and non-state actors continue to grow in importance, with the ability to engage in such activities as espionage, financial theft, and other cross-border crimes sometimes referred to as cyber warfare. The international legal system is attempting to hold actors accountable for their actions, with the International Criminal Court among the few addressing this threat.[20] Computer crime or cybercrime encompasses a broad range of potentially illegal activities.

2.2 TYPES OF CYBER CRIMES

There are many types of cyber crimes, for the purposes of this paper the author will only sample a few since the focus of the paper is different.

2.2.1 Spam

Spam is the unsolicited sending of bulk emails[21] for commercial purposes. This is unlawful to varying degrees. Spamming is the act of sending unsolicited messages to many users at a time, possibly up to thousands, with the usual intention of advertising products to potential customers. Spamming can also be used as a form of irritation by singling out an email address and sending the owner of that address hundreds of emails per second. Spamming is usually random and untargeted though at times it can be targeted at a group of people or the whole community.

2.2.2 Hacking

Hacking involves penetrating a secure area by subverting its security measures. Hackers might accomplish this by setting up programs like "war dialers" that try thousands of common passwords until one is accepted. A hacker may set up "packet sniffers," programs that scan data

[20] Ophardt, Jonathan A. "Cyber warfare and the crime of aggression: the need for individual accountability on tomorrow's battlefield" Duke Law and Technology Review, (2003), p. 1

[21] Types of Cyber Crime, Sponsored by: Forensic Science http://www.spamlaws.com/types-of-cyber-crime.html) visited12/09/2010

from the target system's network ports to find out more about a network and penetrate it more easily. Once hackers penetrate the servers that host their target's computer systems, they can alter or remove files, steal information and erase the evidence of those activities. While many hackers break security systems just out of curiosity, other hackers, however, have attempted to use their skills for illegal personal financial gain.[22]

Breaking into a system is one thing, but breaking into a system without getting caught is a completely different thing. Every attacker strives to be able to break into a system without leaving any traces behind. One method of doing this is by changing one's identity before attacking the target system. Such a strategy not only ensures that an attacker remains anonymous, however, it also opens up a number of different loopholes (like trust relationships) that cannot be exploited otherwise.[23] Thus, identity attacks have slowly but surely become a very common phenomenon.

It is quite clear that no attacker likes to get caught. The best strategy that an attacker can adopt to not get caught is to exploit identity thefts or identity hijack attacks. Such identity hijack attacks not only ensure that an attacker does not get caught, but it also allows an attacker to pass the blame onto an innocent person and through the investigators off the track.[24] Moreover, with the advent of the internet in every home and office, a high number of privacy concerns have also come up. As a result, every regular internet user has to take precautions to protect their privacy.

2.2.3 Piracy

Piracy involves the illegal reproduction and distribution of software applications, games, movies and audio CDs. This can be done in a number of ways. Usually pirates buy an original version of a software, movie or game and illegally make copies of the software available online for others to download and use without the notification of the original owner of the software. This is known as internet piracy or warez. The term "warez" describes commercial software, movies and games that has been modified by a cracker and made freely available to the public on the

[22] Jonathan Zittrain, Charles Nesson and Lawrence Lessig: Internet Law: Foundation Press
[23] Fadia A, An Ethical Hacking Guide to Corporate Security, Macmillan India Ltd: Delhi (2006), pg 99
[24] Fadia A, An Ethical Hacking Guide to Corporate Security, pg 100

Internet. [25] This particular form of cybercrime may be the hardest of all to curb as the common man also seems to be benefiting from the crime. A typical African person would stop at nothing to download "free software, musicals, movie" or related items to make a living.

2.2.4 Computer Viruses

Computer hackers are digital age criminals that can bring down large infrastructures with a single keystroke emitting a computer virus. These types of viruses are macro or binary. Macro viruses attack a specific program, while binary viruses attack data or attach to program files. Hacking into a business's intranet and uploading viruses to the code are examples of these types of crimes. Private citizens are targets of computer viruses when visiting websites with encrypted viruses or opening emails infected with viruses. One of the most famous computer viruses is the Trojan virus.[26]

2.2.5 Cyberterrorism

Cyberterrorism is the adaptation of terrorism to computer resources, whose purpose is to cause fear in its victims by attacking electronic resources. Cyberterrorism is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear.[27]

2.2.6 Online harassment

Online harassment is unwanted contact by offenders that may negatively impact a victim's livelihood, well-being, and mental or emotional state. One of the most common forms online harassment takes is that of cyber stalking.[28] In the loosest sense of the term, cyber stalking is

---

[25] F.A. Longe, The Design of An Information-Society Based Model For the Analysis of Risks and Stresses Associated Risks Associated with Information Technology Applications :Unpublished M. Tech. Thesis, FUT, Akure, Nigeria (2004)

[26] Kerrie Main, Examples of Cyber Crime: April 14, 2010 (http://www.ehow.com/list_6307677_examples-cyber-crime.html) visited 15/09/2010

[27] Denning, D. Cyberterrorism. Testimony before the House Terrorism Committee on Armed Services, May 23, 2000, from:(http://www.cs.georgetown .edu/~denning/infosec/cyberterror.html) visited 13/09/2010

[28] Michael Kunz & Patrick Wilson; Computer Crime & Computer Fraud; University of Maryland, Department of Criminology and Criminal Justice, (Report to the Montgomery County Criminal Justice Coordinating Commission) (2004), p. 19

using a computer in the perpetration of the traditional crime of stalking. The traditional crime of stalking usually involves harassing and threatening behavior that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving messages or objects, or vandalizing a person's property.[29] Cyber stalking involves the use of a computer in the perpetration of those acts.

2.3 UNDERSTANDING THE CONCEPT OF CYBERCRIME

Generally speaking, computers play four roles in crimes: They serve as objects, subjects, tools, and symbols.[30] Computers are the objects of crime when they are sabotaged or stolen. There are numerous cases of computers being shot, blown up, burned, beaten with blunt instruments, kicked, crushed and contaminated.[31] The damage may be intentional or unintentional. Computers play the role of subjects when they are the environment in which technologies commit crimes. Computer virus attacks fall into this category. When automated crimes take place, computers will be the subjects of attacks. The third role of computers in crime is as tools enabling criminals to produce false information or plan and control crimes.[32] Finally, computers are also used as symbols to deceive victims. In a $ 50 million securities-investment fraud case in Florida, a stock broker deceived his victims by falsely claiming that he possessed a giant computer and secret software to engage in high-profit arbitrage. In reality, the man had only a desktop computer that he used to print false investment statements. He deceived new investors by paying false profits to early investors with money invested by the new ones.[33]

In the United States, police departments are establishing computer crimes units, and cybercrime makes up a large proportion of the offences investigated by these units. The European Union has created a body called the forum on Cybercrime, and a number of European states have signed the Council of Europe's Convention on Cybercrime treaty, which seeks to standardize European laws concerning cybercrime.[34]

---

[29] Kunz Michael & Patrick Wilson, Computer Crime and Computer Fraud; University of Maryland, Department of Criminology and Criminal Justice, Report to the Montgomery County Criminal Justice Coordinating Commission (2004), p.20

[30] Mohamed Chawki; A Critical Look at the Regulation of Cybercrime: A Comparative Analysis with Suggestions for Legal Policy; LL.B (1998) p. 8

[31] Mohamed Chawki; A Critical Look at the Regulation of Cybercrime., p. 8

[32] In fact criminals may use computers, graphics software, and colour printers to forge documents. Criminals who create automated crime software and those who purchase and use the software will be using their computers as tools to commit crimes

[33] D. Parker, Fighting Computer Crime: For Protecting Information (U.S.A, John Wiley), [1998] p. 10.

[34] Mohamed Chawki; A Critical Look at the Regulation of Cybercrime, p. 8

When speaking about cybercrime, it is usually spoken about in two major categories of offences. In one, a computer connected to a network is the target of the offence; this is the case of attacks on network confidentiality, integrity and or availability.[35] The other category consists of traditional offences such as theft, fraud, and forgery which are committed with the assistance of/or by means of computers connected to a network, computer networks and related information and communications technology.[36] Cybercrime ranges from computer fraud, theft and forgery to infringements of privacy, the propagation of harmful content, the falsification of prostitution, and organized crime.[37]

One of the factors that make a hard-and-fast definition of cybercrime difficult is the jurisdictional dilemma.[38] Laws in different jurisdictions define terms differently, and it is important for law enforcement officers who investigate crimes, as well as computer network administrators who want to become involved in prosecuting cybercrime that are committed against networks, to become familiar with the applicable laws.[39] Thus, the definition of cybercrime under state law differs, depending on the state. Cybercrime in a narrow sense may mean any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them while in a broader sense cybercrime is any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.

2.4 HOW ARE THE CRIMES COMMITTED?

Understanding the enemy is an essential component of successful defense. Like a general planning fortifications, a security manager must understand black hat tools and techniques and use this knowledge to design countermeasures into the information defense frameworks. Cyber criminals usually go through five key systematic steps when planning to commit a cyber crime.[40]

---

[35] R. Spinello, Regulating Cyberspace: The Policies and Technologies of Control (U.S.A, Spinello), (2002) p. 207.
[36] M. D. Goodman and S. Brenner, The Emerging Consensus on Criminal Conduct in Cyberspace (Oxford, International Journal of Law and Information Technology), [2000] Vol. 10, n. 2 p. 3.
[37] M. D. Goodman and S. Brenner, The Emerging Consensus on Criminal Conduct in Cyberspace, p.3
[38] D. Shinder, Scene of the Cybercrime (U.S.A, Syngress), [2002] p. 6
[39] D. Shinder, Scene of the Cybercrime, p.6
[40] Tom Olzak, The five phases of a successful network penetration: December, 2008, (http://www.techrepublic.com/blog/security/the-five-phases-of-a-successful-network-penetration/701) (visited: Oct. 6, 2010)

2.4.1 Reconnaissance

This refers to the preparatory phase where a cyber criminal gathers as much information as possible about a possible target before launching an attack. In order for the cyber criminal to gather information about the target he wants to attack, he will use some reconnaissance techniques. There are two reconnaissance techniques in use.[41] These are passive and active reconnaissance.

Passive reconnaissance[42] is when the cyber criminal does not directly interact with the system to gather important information about the target. This strategy uses social engineering and dumpster diving. In computer security, social engineering is a term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures. For example, a person using social engineering to break into a computer network would try to gain the confidence of someone who is authorized to access the network in order to get them to reveal information that compromises the network's security. The person may reveal important information like passwords to company systems like payroll or indeed email addresses of key people in the company. This information will then be used by the cyber criminal for hacking. Another area of social engineering is ability of the cyber criminal to easily guess the passwords of users and log onto the system. Most people use their names, dog's names, children's names for their passwords. These can easily be guessed by cyber criminals nearer to them.

Dumpster diving is looking for treasure in someone else's trash bin. In the world of information technology, dumpster diving is a technique used by cyber criminals to retrieve important information that could be used to carry out an attack on a computer network. Some of the information that is gathered through dumpster diving includes usernames, access codes or passwords written down on pieces of paper, telephone numbers, organization charts and many other things.

[41] Tom Olzak, The five phases of a successful network penetration
[42] Tom Olzak, The five phases of a successful network penetration

Active reconnaissance is when the cyber criminal directly interacts with the target system or computer network to collect important information which he will use for cyber attack. The attack may probe network devices, servers and other systems in order to obtain information such as open ports, locations of systems, Internet Protocol Addresses of hardware devices[43] etc.

2.4.2 Scanning

During this phase, the cyber criminal uses the information gathered during reconnaissance to identify specific vulnerabilities. These identified vulnerabilities are then exploited during the actual attack. Scanning is sometimes considered an extension of reconnaissance. Cyber criminals make use of specialized automated networking tools like war dialers, network scanners, trace route, port scanners to determine vulnerable (loopholes) areas in the systems.[44] These tools usually reveal hundreds of loopholes on networks and organizational systems which gives the attacker a great deal of advantage.

2.4.3 Gaining Access (Cyber Attack)

This is the phase where the cyber criminal penetrates into the system illegally to cause damage, steal information, modify accounts, introduce viruses, deny users a particular service or indeed shut down the system altogether. A cyber attack is usually carried out in three ways namely outside the network, internally by logging in using a username and password for the authorized user and through the internet. The cyber criminal can sit outside a network and launch an attack on it through the router until he gains access. Using their special attacking tools, they can also obtain hidden usernames and passwords for various company employees and log on normally on systems and then cause damage. The internet has brought connectivity among nations, organizations and companies for sharing information. However, the internet is also being used as a medium for cyber criminals to penetrate into private networks and systems which include banks.[45]

---

[43] Tom Olzak, The five phases of a successful network penetration
[44] Tom Olzak, The five phases of a successful network penetration
[45] Tom Olzak, The five phases of a successful network penetration

2.4.4 Maintaining Access

Once an attacker has gained access to the network or to a system, they usually retain ownership of the system by continuously disguising themselves while causing serious damage to the system. Cyber criminals have the ability to remain on the system without being recognized for a very long time. They may also be entering into the system but coming out through backdoors so that Information Technology Administrators fail to notice them. While on the system, cyber criminals can use Trojan Horses[46] (special software that installs itself in the background) to transfer usernames, passwords, change bank accounts, credit card information and even crushing the system altogether.

2.4.5 Covering Tracks

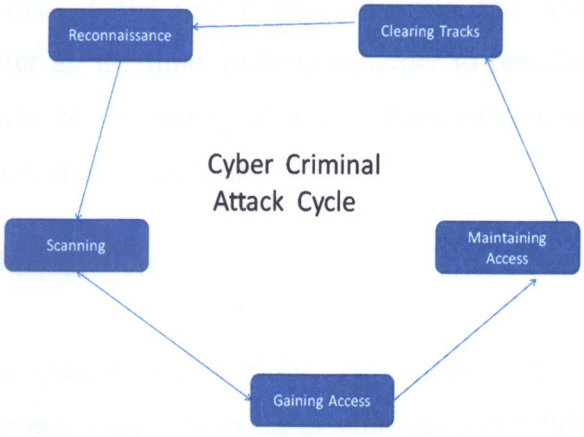
This is the last phase in cyber criminal attack strategy in which the cyber criminal destroys evidence of his attacks from would-be investigators in the wake of evading prosecutions and police arrests. The tools that cyber criminals use to hide their identity include special Trojan horses which have the capacity to destroy evidence from log files. Log files are special files on every system which keep a track record of the users, when they logged into the system, for how long have they been on the system, what they were doing on the system, dates and time etc. Cyber criminals usually edit or destroy the records in the log files by using Trojan horses and hence they cannot be detected or traced at all.

Sometimes, the cyber criminals hide their identity by using root kits. A root kit is software that enables continued privileged access to a computer while actively hiding its presence from administrators by subverting standard operating system functionality or other applications. Once a root kit is installed, it allows an attacker to mask (hide) the ongoing intrusion and maintain privileged access to the computer by circumventing normal authentication and authorization mechanisms. When a root kit is installed, a number of critical system files are replaced in seconds thus hiding the cyber criminal. Cyber criminals have also used a technique called

[46] Tom Olzak, The five phases of a successful network penetration

steganography.[47] Steganography is the technology of hiding information in form of pictures, videos or sounds. Cyber criminals use these for hiding their identity so that they cannot be traced by Systems Administrators.[48]

Here below is an illustration of the stages criminals go through when committing cybercrimes.



2.5 WHY DO PEOPLE COMMIT CYBER CRIMES?

Computer crime comes in many different varieties. As new computer technologies are made available, there is sure to be someone lurking in the cyber-shadows who is ready to exploit, test or take advantage of security holes that may exist. Computers are so prevalent now that computer crime has become the most widespread criminal activity in the world. But what motivates someone to attempt or commit computer crimes?

The motivations for hacking are numerous. Understanding these factors leads to a much clearer perspective on what defenses need to be put in place to mitigate risk. The internet still has many unaccountable regions today, and it is fairly easy to launch attacks with little fear of being traced. Web hacking in particular is easily laundered. Web attack techniques are fairly easily understood, even by the layperson. This makes manipulating application input fairly trivial.[49]

---

[47] Tom Olzak, The five phases of a successful network penetration

[48] Scambray J., Liu V., Sima C., Hacking Exposed Web Applications: Web Application Security Secrets and Solutions, 3rd Ed., Tata McGraw Hill Education Private Ltd: New Delhi (2011), pg 9

[49] Scambray J., Liu V., Sima C., Hacking Exposed Web Applications: Web Application Security Secrets and Solutions,9

Some of the reasons cyber crimes are committed are given here below.

2.5.1 Ease of Anonymity[50]

Computer crime has risen at an astronomical rate, in large part due to the ease with which a perpetrator can remain undetected or anonymous. It is much easier to get away with criminal activity in a cyber world than in the real world. However, the ability to track IP network addresses is becoming greater all the time, making it harder to remain invisible when online.[51] Still, there is a strong sense of anonymity that can draw otherwise respectable citizens to abandon their ethics in pursuit of personal gain.

2.5.2 Inadequate Legal Jurisdiction

Computer networks literally span the entire globe. This makes it virtually impossible for any government or law-enforcement agency to enact or enforce laws when computer criminals are set up in foreign countries. In many cases, computer criminals are actually backed by their local governments, in an attempt to carry out computer espionage or cyber-terrorism. These criminals are able to perform their computer crimes out of a sense of duty to their respective countries, and are able to do so without any fear of arrest or apprehension[52] because they know that they will not be traced.

2.5.3 Old Crime, New Technology

Many computer criminals use their computers merely as a logical extension of "traditional" crimes that can take advantage of computer technology to help facilitate or carry out the crime. Crimes such as child pornography, identity theft and money scams are in many cases made easier by the use of a computer. Automated software can be programmed to steal credit card numbers, personal identification information and even cellphone codes.[53] By stealing personal information, a computer criminal may attempt even more serious criminal activity under the stolen identity.

---

[50] Scambray J., Liu V., Sima C., Hacking Exposed Web Applications: Web Application Security Secrets and Solutions, pg 9

[51] Bobby Stocks; Why Do People Commit Computer Crimes: June, 2009, (http://www.ehow.com/about_4709031_do-people-commit-computer-crimes.html) site visited on Oct. 6, 2010

[52] Bobby Stocks; Why Do People Commit Computer Crimes

[53] Mary Krenz; Cyber Crime - A New Way to Commit Old Crimes: 2004, (http://ezinearticles.com/?expert=Mary_Krenz) accessed on Oct. 6, 2010

2.5.4 Holding a Grudge

Malicious computer codes like worms and viruses are often spread by someone who is seeking to cause harm to an individual or company possibly over losing a job, perceived unethical business conduct or maybe even jealousy or envy.[54] Such parties intend to destroy or cripple their targets for the personal satisfaction of seeing them suffer the effects.

2.5.5 Thrill of the Game

For many computer criminals, the excitement and challenge of exploiting a computer system can be too great to resist. Computer gurus are notorious for gleaning information about specific networks and software designs that they have an irresistible urge to put to a test. Unfortunately, much of this information translates into illegally compromising computer systems in one way or another. Still, the lure of "cracking the code" will continue to be a major factor in enticing some to commit computer crimes.[55]

To sum up on this chapter, the author wishes to indicate that the capacity of human mind is unfathomable. There is no limit to the way a human mind can think but it is in our hands to take precautions to prevent falling prey to such insidious acts. It is not possible to eliminate cybercrime from the cyberspace completely. It is quite possible to check them. History is the witness that no legislation has succeeded in totally eliminating crime from the globe. The only possible step is to make people aware of their rights and duties (to report crime as a collective duty towards the society) and further making the application of the laws more stringent to check crime and punish the few that are caught very severely.

[54] Bobby Stocks; Why Do People Commit Computer Crimes
[55] Bobby Stocks; Why Do People Commit Computer Crimes

CHAPTER THREE

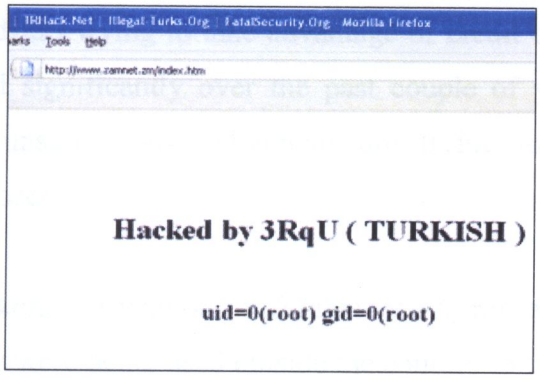
3.0 PREVALENCE OF CYBER CRIMES IN ZAMBIA

The prevalence of cybercrimes in Zambia cannot be over emphasized as noted from the then Communication Authority Acting Controller, Richard Mwanza's statement when he called on internet service providers to make security an important feature of their service so as to protect customers from the risk of viruses and other attacks that might lead to loss of important personal and confidential data as way back as 2008 when ZAMNET- Zambia's leading Internet Service Provider, (http://www.zamnet.zm) was hacked. Even though the prevalence rate is low, cybercrime are actually being committed in Zambia as will be shown from the case study below. The site was hacked on Saturday the 27th of December, 2008. The Hackers who called themselves 3RqU (Turkish) changed ZAMNETs landing page. The hackers gained unauthorized access to ZAMNET servers. According to the new landing page that had been put on ZAMNET, the hackers claimed to have root access. Root access grants someone the ability to control all the resources on a server. With this access hackers can for example delete the whole server, read all confidential information on the server or make alterations on the site.

Most of the websites hosted by ZAMNET were affected by this security breach and these included sites like Times of Zambia, Daily mail, Zambia National Broadcasting Corporation to mention but a few. According to some experts ZAMNET was using an old version of a web server though it was noted that, that might not necessarily be the cause of the breach but rather the lax in ZAMNETs policy on applying security updates to the software on their servers. Mr. Mwanza urged Internet Service Providers in the wake of the hacking of ZAMNET web server to make security an important feature of their service. He said Service Providers needed to protect the customers from fraud and thefts that may arise as a result of sharing personal information online.

The figure below shows how the landing page of the ZAMNET website looked like when it was hacked in December, 2008.

Zambia's Leading ISP Hacked



Clearly, the hacking of ZAMNET web server shows how vulnerable Zambia is to cyber criminals and this should not be taken lightly because ZAMNET customers lost business whose cost could not be quantified and eroded the confidence in people who trusted in information communication technologies. This is the harm that cybercrime can cause either to an individual, a business corporation or indeed a government system hence the need to put in place mitigation procedures that should ensure business continuity in the case of any eventuality.

3.1 THE STATUS OF THESE CRIMES IN ZAMBIA (CASE STUDY)

3.1.1 Thefts on Automated Teller Machines (ATMs)

Zambia hit by alleged debit card fraud[56]

ATM Machine

[56] By The On Line Post Newpaper of Thursday 29 July 2010

Zambia hit by alleged debit card fraud made headlines in both the print and electronic media in July, 2010. Some retail customers in the country reported suspicious debit card transactions on their accounts a situation that had caused panic among some local debit card users. This is the problem that goes with fraudsters trying to take advantage of credit or debit cards. With cards, and ATMs having increased significantly over the past couple of years from 80 in 2005 to currently over 400, some unscrupulous individuals are trying to take advantage of this development in the financial sector.

Initial investigations by Bankers Association of Zambia (BAZ) revealed that some cards could have been replicated and they were being used outside the country to transact on both Automated Teller Machines (ATMs) and points of sale. Bankers Association of Zambia Chairman Saviour Chibiya said the problem of cyber crime involving bank payment system was not unusual in other markets where the financial sector was more developed than Zambia.

These cybercriminals harvest the information usually at the point of making a payment as they have technology which can read information from someone's card and replicate it. That is why it is important to try not to let the card out of sight when making a payment. However, it is not only a Zambian issue as electronic funds transfer systems have been proliferated world over and transactions intercepted and diverted. Valid credit card numbers can be intercepted electronically. The digital information stored on a card can be counterfeited as what happened in 1994, when a Russian hacker Vladimir Levin, operating from St Petersburg, accessed the computers of Citibank's central wire transfer department, and transferred funds from large corporate accounts to other accounts which had been opened by his accomplices in The United States, the Netherlands, Finland, Germany, and Israel. Officials from one of the corporate victims, located in Argentina, notified the bank, and the suspect accounts, located in San Francisco, were frozen. The accomplice was arrested. Another accomplice was caught attempting to withdraw funds from an account in Rotterdam.[57]

[57] Sheryll Lim-Robrigado, Poetic Justice: Cybercrimes, Electronic Money Laundering and Tax Evasion, (2009) http://sheryl-lim-robrigado.blogspot.com/2009/11/cyber-crimes.html visited 21/09/2010

Zambia has not been spared of these crimes. Most card users were sent into panic as the email below circulated warning card holders to be cautious when buying using their cards. (The names of institutions and the author have been removed for security reasons.)

> "Dear All,
>
> Please be notified that there is ATM card fraud taking place in Lusaka. I did my shopping at XXX (Mall) and I used my ATM card using the XXXX (Bank) machine. After a day I discovered I had lost a lot of money and my details on my ATM card were being used in SA to purchase grocery at any grocery shop there.
> This fraud is being investigated now by Police Headquarters and those affected are holders of XXX Bank clients. This also happened to a friend of mine who works for XXX - Woodlands. She used the ATM card for shopping at the same shop and lost 9million kwacha after a day of shopping from her account. Please note even other banks may also be affected.
> I would like to encourage all of you to use cash when you want to purchase groceries in a shop to avoid what happened to me and my friend.
> Best Regards
>
> XY."

There are some cases that have been reported involving thefts on ATMs. In the case of **The People v. Charlie Tommy and 5 Others**[58] which involved six suspects, being; Charlie Tommy, Buster Mudenda, George Chilufya Mubanga, Kenny Mushimba, N'gandu Hakalima and Andrew Kawana Simbotwe where these men had devices such as laptop computers, printer, an electronic card reader and some used and unused visa and master cards suspected to have been made by themselves managed to capture data from clients' cards and used such data to steal from the clients' bank accounts.

Charlie Tommy the mastermind was of foreign nationality, a Namibian who recruited the others into this crime activity. This illustrates the fact that cyber crime can be committed across borders and that the criminal need not be in the particular jurisdiction where the crime activity is carried out. This therefore calls for concerted efforts between and among states in order to minimize the commission of these crimes. To give more insight on this, the brief facts are that one of the defendants, N'gandu Hakalima a Hotelier/Auditor at Ridgeway Sun Hotel, Lusaka is the person who was given the gadget which was being used to steal (capture) personal information from unsuspecting clients who would make payment either by using a credit, visa or

[58] CRMP-18-2010

master card. This is achieved through the process called swiping of the card when making a payment. The information so obtained by Hakalima was passed on to the others and eventually make their own self-styled cards and put on that information obtained illegally and they would thus pose as genuine cardholders either at the shops or any trading house where they allow payments by credit, visa or credit cards and purchased assorted expensive goods.

In this case, the victims were three South Africans who had checked in at Ridgeway Sun Hotel, Lusaka for about three days. Their personal banking details were stolen at the time they were checking out because they paid their bills using their cards such that when they got back to South Africa they were amazed when their respective bankers phoned them inquiring why they were spending their money in a very unusual manner. But they all declined having spent much when they were in Zambia except at the Hotel. Their bank statements indications highlighted a number of transactions to the effect that they had bought items from Mr. Price (Zambia), Wool Worths Manda Hill, My Choice Manda Hill, Cosmic Computer Suppliers, Shoprite (Zambia), Radian Stores and some other shops.

Investigations were carried out and the first clue to this crime pointed to Ridgeway Sun Hotel, Lusaka where the Hotelier who checked them out was identified as having been given their cards as they made payment for their respective hotel bills. The suspects were jointly charged with the offences of making documents without authority, theft, obtaining goods by false pretences, possession of electronic devices and unauthorized access to and interception of or interference with protected data.

In a similar incident, a tourist from the United States of America (USA) came to Zambia and lodged at Hotel Intercontinental for three days and when checking out he used his visa card to pay for the hotel bills. When he went back to the USA he was shocked to discover, to his dismay that his bank statement was showing that he had bought three air tickets from Ethiopian and also from Zambezi Airlines when he was in Zambia[59].

[59]Interview with Mr. Mukuka Chileshe - Supervisor for Financial and Computer Fraud Investigations at the Police Headquarters on 17/01/2011
* The names of the victims have been withheld for security reasons. Suffice to mention however that these are true cases that have been reported to the Police.

Another case involved a Zambian woman who had gone to South Africa and while at Thabo Mbeki Airport, she admired some item which she purchased using her visa card. When she came back home, she discovered that her bank statement was showing that while in South Africa she had done extensive shopping from a varied range of shops and not only from the airport where she had bought only one item.

Locally, there were a number of people who were affected especially during the July, 2010 thefts though some people did not report these cases to the police some due to the fact that they did not know maybe because the amount was not very big or they just didn't know that something wrong had been done in their account. There are, however a few (about four) that were reported involving loss of these amounts; K5m, K2m, K8.5m and another one for K58.8m. The circumstances in all these cases are similar. They involve situations after someone withdraws money using their visa card and the next moment they discover irregular transactions purporting to have been conducted by them in places where the person had not even gone to in some cases.[60] This point qualifies the fact that cybercrime is no respecter of jurisdiction. It can be perpetuated by a person in a totally different jurisdiction altogether.

Besides the kind of theft where a card is duplicated, some crimes on the ATMs involve situations where the card holder is just careless with his or her card. The Zambia National Commercial Bank[61] experienced a case in Chipata, where a wife stole her husband's card and sent a friend to go and withdraw money for her. Another case involved a daughter who over a period of time withdrew over K50million from her father's account. The daughter had once been sent to withdraw money using the card and then she mastered the pin number and when the father was unsuspecting she would steal the card and withdraw money and secretly take the card back. Generally speaking, cases of this nature should be plenty only that they are not reported for fear of souring relationships, so they just end up at family level and are forgotten.

[60] Interview with Mr. Mukuka Chileshe
[61] Interview with Mr. Musonda Kapaya – Chief Information Security Officer at ZANACO Head office on 31/01/ 2011

3.1.2 Phones (Cellphones and Landphones)

The use of cell phones is one thing that has cheered the Zambian populace as it has made communication far much easier than before. Business transactions are conducted with relative ease because people can freely link up at any time and from any place without necessarily depending on the office landline as before. This however, is by no means intended to suggest that land phones are no longer useful.

Just as legitimate organizations in the private and public sectors rely upon information systems for communications and record keeping, so too are the activities of criminal organizations enhanced by technology. There is evidence of telecommunications equipment being used to facilitate organized drug trafficking, gambling, prostitution, money laundering, child pornography and illegal trade in weapons.

Telecommunications systems can also be used for dissemination of offensive materials and for harassing and threatening like in the Zambian case of, **The People v. Oscar Chizanda**[62], where Mr. Chizanda was convicted for written threats to murder by using a cellphone. The brief facts of the case are that the accused person (Mr. Chizanda) was writing threatening messages to a man he suspected as having an affair with his wife. It is worthy to note here that such nature of the crime is very common the only thing is that the crimes are normally not reported.

[62] SSP-20-2007

Another case which involved the use of a phone is the case of **The People v. Chibuye Mwanje**[63]. In this particular case, Chibuye between 25th and 29th May, 2009 knowingly did cause Patricia Daka Jere to receive written threats that she would be murdered contrary to section 218 of the Penal Code Chapter 87 of the Laws of Zambia. She sent her many threatening text messages on the phone and also phoned her to issue the same threats. She was convicted of the offence.

There are also instances where calls have been tapped and people's private conversations listened to by people who are not supposed to listen to such conversations. Developments in telecommunications sector tend to provide new opportunities for electronic eavesdropping. Here again, technological developments create new vulnerabilities.[64] Such cases have also happened here in Zambia; unfortunately they are not on record.

A new mobile spyware program, which has already hit several cell phone users, enables hackers to have complete control of one's phone without their knowledge. In two instances that have been reported, Airtel Zambia airtime worthy K65million was stolen from someone's cellphone and transferred to a different number without the owner's immediate knowledge until later on when he wanted to make a call only to be told that he lacked credit in his phone. In another development, a criminal had access to someone's mobile phone account and managed to transfer Airtel airtime worthy K35million to his phone and to different phone numbers. As a measure to avoid the owners of the cellphones the criminal transferred the airtime to using it, he temporarily blocks those numbers until he removes the airtime from those numbers rendering the owners of the phones incapable of using their phones. He then sells the airtime to his benefit. The criminals were charged with unauthorized access to, interference of, and interception of data contrary to Section 99 (1 and 2) of the Electronic Communications and Transactions Act No. 21 of 2009.

---

[63] 2SP/C/132/09

[64] Cell Phones - Hackers Next Target: MobileIN.com Home Page, 2009 (visited 10/10/2010)

Cell phone threats, while rather recent to come on the scenes, are continuing to emerge at a concerning rate. Malware disguised as multimedia content and worms are being used to infect these devices. These pieces of malicious code cause the leakage of private information and in some cases extra service charges. Cell phone giant Nokia acknowledges the possibility of the threat and says it intends to take all necessary steps to combat it.[65]

The criminals have hacked just about everything else and now they are targeting the cell phones. Cellphone hacking has just recently surfaced. Cellphone hackers have apparently found a glitch in the way the chips are manufactured. The good news, though, is that it only applies to the first generation models of cell phones that use the Global System for Mobile communications (GSM). Another requirement is that the hacker must have physical access to the cell phone for at least three minutes. Currently, although the problem has been remedied in the second and third generation phones, it seems that about 70% of existing cell phones fall within the first generation category. [66] Another way that mobile phone hacking can take place is for a hacker to walk around an area with people that have cell phones and a laptop that has cellphone hacker programs on it. Through an antenna, and a little patience, his computer can literally pick up the cell phone data if it is turned on. This is more applicable to cell phones that use Bluetooth technology.

3.1.3 Electronic Mails (Emails)

Laptop Computer

[65] Kevin G. Coleman of Technolytics ; Cyber Crime Mobile: 2009, P 888-650-0800
[66] Cell Phones - Hackers Next Target, : MobileIN.com Home Page, 2009 (visited 09/10/2010)

Hacking involves penetrating a secure area by subverting its security measures and once hackers penetrate the servers that host their target's computer systems, they can alter or remove files, steal information and erase the evidence of those activities. While many hackers break security systems just out of curiosity, other hackers, however, have attempted to use their skills for illegal personal financial gain.[67]

The hackers are extremely sophisticated people and to an unsuspecting individual their tales are enticing as they would coin their story in highly-enticing promises of lifting someone out of the dungeon of poverty, with a million-dollar announcement that he had become the overnight billionaire through winning the year's billions of dollars raffle draw, for which someone never entered at all like what happened to a woman in Zambezi District who received a message on her mobile phone informing her that she had won £300,000.00 and that she needed to pay some money for administrative purposes; for handling the sending of that huge amount. The victim was being asked for this money in small amounts and after she had sent a total of K25m, communication ended with the people who were promising to send her the money and she just lost out on her money.[68]

Some messages would ask the recipient to contact a freight carrier service provider in some country though often they like using the West African country of Ghana, and the company would in turn demand about US$500 as handling fees. Still some hackers would send a hoax message of appeal to every contact in the address book of a hacked email asking for assistance as what happened to the author's own friend. Exhibited here below is the mail the author received from the fraudsters among other recipients, purporting to be the friend and soliciting for help.

> Thursday, 21 October, 2010 15:21
> **From:** "Florence Chikapa" <flolubasi@yahoo.com>
> **To:** "Sombo Chinyama" sombocollins@ymail.com
>
> *Greetings,*
>
> **Help please**
> *How are you doing today? I am so sorry if my email would bother you, but I want you to please help me out of this devastating situation that I got myself into, I had to come*

[67] Jonathan Zittrain, Charles Nesson and Lawrence Lessig: Internet Law: Foundation Press
[68] Interview with Mr. Mukuka Chileshe

down to UK for a business meeting I could not meetup, unfortunately for me I was attacked by robbers in the Hotel where I lodge along city road in Blackburn. The robbers made away with all my money, entire luggage's and air return tickets, they also disconnected the Hotel's telephone cables.
Please I need you to lend me £1500GBP so I can use it to settle up my Hotel's bills and book the nearest flight home and as soon as I return home I will refund back the money, please I need you to send the money via Western union money transfer to my name and on this address below,
Name: Florence Chikapa
Address: 102 Preston New Rd, Blackburn ,United Kingdom.

Thank you so much, after sending me the money, I need you to email me the scanned copy of the western union receipt or the MTCN numbers, because I did not bring my phone here.
Hope to hear from you soon.
Thank you
fcl

With internet hacking becoming more sophisticated by the day, it is advisable for users of personalised web-based email services such as yahoo, gmail, and hotmail to watch against this growing trend of cybercrime to avoid losing all their important contacts and deals as a result of email accounts being hacked. Nebert Mulenga, an investigative writer recounts how his life almost came to a standstill after his inbox was hacked.[69] It all started on March 19, 2008, with one attempted response to an email that was purported to have been written by a cancer patient in need of someone who could offer to support a 'worthy' cause of the hospitalized patient who wrote in part, "I am writing this mail in pains but with confidence believing that if it is the wish of God for you to help me to carry out these course, God almighty in his infinity mercy shall bless and reward you in abundance. My intention of contacting you is to solicit your humble assistance for a project, which will be mutually beneficial..." went the mail in part.

The purported cancer patient's long story was to entice Nebert Mulenga to send some money to Ghana in order for him to later be sent money by someone who was in charge of her late husband's funds which Mulenga should use for charitable works. When this attempt failed, it marked the beginning of a chain of other syndicates attempting to siphon hundreds of dollars from him. Barely a week after that, another email flew in from a Mr. Marcel Fataumana, announcing that Mulenga had won a total of US$1 million in the "Microsoft 2008 Promotion"

[69] Nebert Mulenga; A Scribe's Encounter with High-Tech Conmen: Times of Zambia Website (2005)

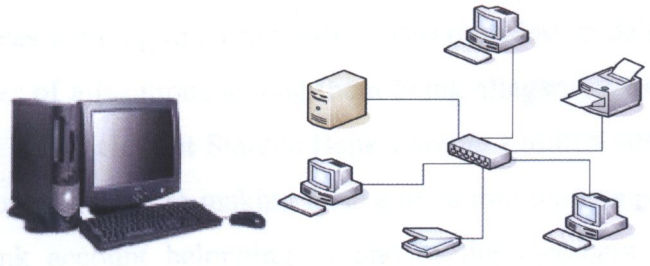
and should claim it in the soonest possible time. When he sent in a 'claim' with the provided details, the response was the same, asking for US$450 handling fee. Then almost two weeks later, another e-mail emerged; this time from a Mr. Sylvester Kabore of Burkina Faso, announcing a cheque of $800,000 was awaiting Mulenga's request, with a fee named at the end of the deal.

Cybercrimes are real in Zambia. Their prevalence especially in connection with the internet use cannot be over emphasized. People's email accounts are being hacked every time and important business connections and information is being lost in the process. In some other incidences, people are being swindled out of millions Kwachas with regard to internet buying. A few cases have been reported to the police concerning people who want to buy cars on the internet. For example in one instance, a Lusaka man was swindled of K380m by an Australian company that deals in second hand cars with agents in the UK when he wanted to buy a benz car. What normally happens in such instances is that when a customer admires a vehicle, he/she will be sent a quotation which will contain the bank details of the selling company through which the buyer has to send the money through the bank. In this case after the buyer transmitted the money sometime in 2009, suddenly there was communication breakdown and up to now he has never received the car. In another case involving the same company, another person was swindled of K700m when he wanted to buy a benz and another car. After transmitting the money, he was promised that the car had been shipped but up to date he has never received the cars and he fails to get in touch with them because they have blocked him from having access to them. In yet another case involving the same company, another person lost $45,000 when he wanted to buy a Nissan Pathfinder which unfortunately, he has never received to date.

The crimes on the internet are gaining ground and so many people are losing money when buying on the internet especially in this area of buying cars, about twelve cases[70] have been reported to the police by people who have been swindled within the past two years. Due to the scope of the paper, the other incidences will not be talked about.

[70] Interview with Mr. Mukuka Chileshe

3.1.4 Computer Systems and Applications



The first recorded case of Internet censorship in Sub-Saharan Africa occurred in Zambia in 1996 when the Zambian government was angered by a newspaper article containing information on then-secret plans to hold a referendum on the country's 1996 constitution and made possession of the offending newspaper edition a criminal offense. They extended their prosecution to the Internet, threatening Zambian Internet Service Provider (ISP) (Zamnet) with criminal charges if the ISP did not take the edition offline.[71]

Zambia's most famous case of cyber-crime involved the hacking of the State House website by a young computer expert, which saw a picture of the then Republican President Mr. F.T.J. Chiluba replaced with a cartoon. The suspected hacker was charged with defaming the head of state, but the case against him failed because there was no law in Zambia to deal with cybercrimes.[72]

Another case showing the status and prevalence of cybercrimes in Zambia is the case where The Drug Enforcement Commission (DEC) arrested a 33-year-old manager at Zain Zambia for hacking into the electronic communication system of Mr. Price, an international chain store operating in Zambia. Mr. Nyawali the DEC spokes person was reported as saying Mercy Lwipa was charged with an offence of unauthorized access to data contrary to section 99 (1) of the Electronic Communications and Transactions Act number 21 of 2009. He said Lwipa hacked into the system with intention to tamper with evidence in the case involving four former employees of Mr. Price who were arrested in 2009 for stealing over K1 billion from the chain store.[73]

---

[71] Sally Burnheim, "The Right to Communicate: The Internet in Africa," Article 19; Sub-Saharan Africa, 2006-2007

[72] This has been written from memory as efforts to trace the case proved futile.

[73] Abigail Chaponda, The Post Newspapers Zambia; November 10, 2010

The People vs Yusuf Pando and Bengula Beyani[74] is yet another cybercrime case which involved the bank's employees working in corroboration with outsiders to defraud the bank. The case involved quite a number of allegations among them being allegations to the effect that one of the accused persons who was a clerk at Stanbic Bank Zambia Limited with intent to defraud on several occasions made or was privy to making false entries into the computer network of the bank into the personal bank account belonging to one of the members of the fraud team purporting to show that on the dates in question amounts of money were deposited into the said account when in fact not. Funds were posted to the accused person's account and later withdrawn in a manner which made the supervisor rule out any misposts.

In **The People v. Dominic Mukuka Tresha, Humphrey Chewe and Nephas Kango**[75], the three accused persons on unknown dates but between 28th April to 5th August, 2008 jointly and whilst acting together knowingly and with intent to commit an offence namely to steal and fraudulently transfer Zain Zambia air time valued at K1,406,278,000.00 to a dealer by accessing programs or data held in the Computer system of Zain Zambia Limited did transfer air time to a dealer fraudulently.

Cybercrimes though seemingly unnoticed, institutions be they public or private, learning institutions like the University of Zambia (UNZA) or otherwise are grumbling with them. UNZA for example has had to deal with issues of illegal changing of results on a number of occasions. In one particular instance in the School of Humanities, the school had written letters congratulating students who had performed well. Later on one student claimed to have been omitted on the list of those that were congratulated. A thorough check revealed that the Assistant Dean in the school at the time had changed to improve his grades. This is possible to be determined because each user of the system is given a username and a password and the system records each user's activities and a log was produced which showed that the said officer had actually tempered with the results.

[74] 2SP. 13.2004
[75] 2SP/C/01/1010

In yet another case involving the same officer is when he changed the results of a girl in the School of Natural Sciences. The student had only passed one course out of four. Upon paying the Assistant Registrar, he changed her results in two courses and the comment from exclude school to proceed. The log in the computer system showed that the results were changed.[76]

Another case involved admission of a student who had not qualified for UNZA admission. The issue surfaced because the other students who were at the same high school with this particular student who was admitted illegal were surprised to find that he had been admitted and so they reported the matter to the Anti-Corruption Commission who investigated the issue only to discover that the Assistant Registrar in the Academic office was paid to alter the results of the student in order to grant him admission into the University.

Another case involving the Assistant Registrar - Academic Office is when he changed the results of his daughter who had been sent on part-time to do one course before she could graduate. He illegally changed her grade from D to C and this enabled her to even graduate. It was later discovered after she had even graduated because the log showed the illegal state of affairs.

It may look like cybercrimes are not there in Zambia just because only a few people use these systems but in reality the crimes are being perpetuated every day. Data is being lost; systems are being hacked; people are losing jobs while others are being swindled on the internet on a daily basis its only that many of these crime activities are not being reported to the relevant authorities. Cybercrimes are here with us all that is required is to put up protective measures in order to protect our systems and personal data from being tempered with by criminals.

[76] Interview with Mr. R. Phiri – Manager Systems Development at the Centre for Information and Communication Technologies at the University of Zambia Main Campus on 26/01/2011

CHAPTER FOUR

4.0 MEASURES BEING CONTEMPLATED BY THE VARIOUS STAKEHOLDERS IN ORDER TO COMBAT CYBERCRIMES IN ZAMBIA

This chapter is designed to look at the measures that the stakeholders, which include the government, have taken or intend to undertake in order to combat cybercrimes in Zambia. After having studied the nature of these crimes and the status in Zambia, it is important to know what is being done about these crimes especially by the government which is the major stakeholder.

4.1 GOVERNMENT RESPONSE

The government has undertaken quite a number of measures in regard to lessening of cybercrimes in Zambia. Some of these are here given below:-

4.1.1 Enactment of Legislation

Enacting legislation is the most important way in which a government can deal with policy matters to put up certain measures and guidelines. In 2004 the government enacted The Computer Misuse and Crimes Act after the encounter of the young computer expert which saw a picture of the then Republican President Mr. F.T.J. Chiluba replaced with a cartoon. The suspected hacker was charged with defaming the head of state, but the case against him failed because there was no law in Zambia to deal with cyber crimes.

The said Act though it satisfactorily helped forestall the frauds that rocked banks and other financial institutions since the emergence of widespread use of computers and other high technological processes in banking, it neglected other important areas. The Computer Misuse and Crimes Act of 2004 was conceived at a time when the use of the internet was not as widespread and diverse as it is today and as such, the law failed to adequately address many issues related to computer crimes. Suffice to say, the Act had a number of inadequacies.[77]

[77] Kapumba N. Doris, Obligatory Essay entitled: The Computer Misuse and Crimes Act of 2004: Its effectiveness in combating cyber crimes in Zambia, (2006) * This is the general view that the author took in her conclusion of the analysis of the said Act.

It is no wonder, the Computer Misuse and Crimes Act of 2004 was repealed and replaced by the Electronic Communications and Transactions Act No. 21 of 2009. This goes to show government's commitment in trying to provide effectively for the fight against cybercrimes.

4.1.2 Promoting Security in the Information and Communication Technology Sector

The emerging trend for increased information access/exchange resulting from integrating ICTs within the social, cultural and economic sphere of the country also brings to the fore a number of security, privacy and consumer protection issues that need to be addressed as part of the efforts of developing an information society. Zambia like most countries in the world is vulnerable to some of the negative implications that may hinder the mainstreaming of ICTs in society. Therefore, specific security measures and mechanisms to ensure the safety of citizens, communities, businesses and the nation at large are needed to minimize negative impacts.[78]

4.1.3 Encouraging Organizations to invest in ICT Security

The Government of Zambia is encouraging companies to make cyber security a priority so as to safeguard data and information resources. According to the Electronic Communications and Transactions Act No. 21 of 2009, it is a criminal offence for a company to fail to secure its network infrastructure. This law coupled with other Government initiatives are now compelling companies in Zambia to consider cyber security as a priority. A number of Zambian organizations have not yet taken considerable steps to invest in cyber security and hence their network infrastructures are vulnerable to cyber attacks. Cyber security is being viewed as a cost even when it is part of the cornerstone to safeguarding scarce data and information resources. Companies are losing millions of money rebuilding network infrastructures vandalized by cyber criminals while other companies are grappling with the complicated task of refunding genuine clients whose accounts have been hacked. These kinds of situations would greatly be avoided if organizations, companies and other groupings invest in cyber security.

[78] National Information and Communication Technology Policy; Ministry of Communications and Transport (April, 2006), p. 17

4.1.4 The Creation of the Zambia Information Communication Technology Authority

Zambia Information Communications Technology Authority (ZICTA) is a government institution that is responsible for regulating the ICTs and developing standards for various ICT thematic areas. They also allocate spectrum to various operators thus the role of ZICTA is that of regulation. Being a regulator, ZICTA has power to deregister an ICT Company that is not following the operational code of conduct. If a company commits a cyber crime, ZICTA is greatly empowered to deregister that company. In this way ZICTA as an arm of the government is helping in the fight against cyber crimes. An example to this fact is when ZICTA, then Communications Authority intervened when Zamnet's system was hacked in 2008 by calling upon the Service Provider to ensure that their system was secure in order to protect their clients' information. Similarly ZICTA recently intervened in the case of Emmanuel Mwamba's where he is accused of authorship of a contemptuous article by giving evidence against the accused in the matter.

4.1.5 Formation of the National Working Group/Committee on Cybercrimes

The government has put in place a committee of professionals in ICTs to plan various strategies for combating cyber crimes in the Country. This committee is also there to protect Zambian Organisations from cyber predators so that Zambia continues to be attractive to investors. Furthermore, the committee works as an advisory body to the Government and all the investigating wings (Zambia Police Service, Anti-Corruption Commission, Drug Enforcement Commission) of Government on cyber crimes. Zambia Information Communication Technology Authority (ZICTA) also uses the Committee for cyber crimes awareness campaigns to parastatals and the corporate world.

4.2 THE FINANCIAL SECTOR

When the country experienced frauds on the ATMs in July, 2010 the Banks worked tirelessly to try and restore the confidence of their clients and put up emergency measures to minimize the commission of the crimes. According to Standard Chartered Bank's Head of Corporate Affairs

Luke Njovu the Bank had managed to contain the alleged cyber crime and suspended transactions in twenty-one (21) foreign countries.

The Banker's Association of Zambia Chairman at the Time, Mr. Chibiya advised people not to let their cards out of sight when making payment because the cyber criminals harvest the information on the cards usually at the point of making a payment as they have technology which can read that information from someone's card and replicate it.

In order to protect the customers' funds and to ensure that customers are not inconvenienced, a number of Banks had taken various protective and preventive measures. Some banks blocked certain countries while others have reduced transaction limits in certain countries. For example, Standard Chartered Bank has blocked card transactions in 21 high risk countries. The Bank has further reduced the limit from USD2,000 to USD200 for all non-Standard Chartered Bank card transactions. Further the Bank has blocked all transactions on some cards where a suspicious transaction had been identified and issued replacement cards to the customers. Other measures that the Bankers Association of Zambia advised customers are to continue observing the security tips given by the respective banks when they open accounts and when collecting ATM cards. Among these include, carrying of cards separately from the wallet in a zippered compartment or a business card holder, or another small pouch, keep an eye on one's card during the transaction and get it back as quickly as possible, save receipts to compare with billing statements in case of purchases using the cards, open bills promptly and reconcile accounts monthly, report any questionable charges promptly and in writing to the card issuer and notify card companies in advance of a change in address. Card users are also advised to not to lend their card(s) to anyone, not to leave their cards or receipts lying around, and not to sign a blank receipt in advance, not to write their account number on a postcard or the outside of an envelope and not to give out their account number over the phone.

Other measures which are long term in nature include the installation of cameras on the ATMs. Some of these machines already have cameras aimed at capturing the face of the person transacting so that in case of dispute like in the case cited above where a woman stole her

husband's card, if that particular ATM had a camera, it would have shown the face of the one who withdrew the money. Though to the contrary, criminals also take advantage of the same facilities to capture information from the card and especially the pin number because the camera will show which keys the customer punched and then replicate the card for their illegal purposes.

The financial sector is undertaking awareness sensitization to educate their clients on generally how to transact especially on the ATM. Things like not to ask for help from a stranger unless one is sure that the stranger is a bank employee, not to expose their cards anyhow and many other safe guards like the ones given above.

Other measures being contemplated by the Banking sector include the installation of anti skimming devices on the ATMs that are meant to protect the information on the card from being skimmed so as to be duplicated. In the long term, ZANACO[79] is considering migrating from the magnetic strip visa cards to chip visa cards which have more security features that are difficult to copy. Currently in Zambia we are using the magnetic strip cards which are open and easily readable.

Further, banking institutions are putting up administrative measures to try by all means possible to minimize these crimes because in the majority of these cases involving ATM cards, there is corroboration between employees of the bank and criminals out there. One such safe guard is to separate responsibilities among employees to avoid having the same person or group of persons for example issuing the cards to customers and at the same time issue them with the pin mailers. The ideal situation now is that these responsibilities will be handled by different people. There is an incidence which occurred in Kabwe that involved an employee of a bank who was unfortunately carrying out both duties; the issuing of cards and the pin mailers at the same time. The employee took advantage of his office and started withdrawing money from three accounts of customers who had not collected their cards. It so happened that one of the three clients was a

[79] Interview with Mr. Musonda Kapaya – Chief Information Security Officer - Zambia National Commercial Bank Headquarters, Lusaka on 31/01/2011

police officer who by that time had gone to Sudan on peace keeping mission; hence his not collecting the card. When he came back to Zambia, the card he had, had even expired but his account had been reaped off all the money and the statement reflected that he had withdrawn the money through using his ATM card. An investigation revealed that one of the bank's employees was responsible for the crime. Therefore, separation of some duties will help tremendously to counter the commission of these crimes.

Installation of antivirus software that is able to detect virus and flush them out of the system to secure the information on the systems is another control being taken in this sector. Of equal importance too is the installation of fire walls. The fire wall will censure the type of information and certain websites that should be accessed through the system such that unauthorized information or access to certain websites which are not authorized is denied. This helps protect the system of an institution from attacks and consequent loss of vital data.

The banks also have measures to control access to certain places especially within their buildings. This to a certain extent prevents access to data by criminal who will find it difficult to gain access to the information unless they are working with an insider. For example they have intrusion detective systems that do monitoring by cameras and intrusion prevention which virtually restricts entry to unauthorized persons. Generally, these are some of the measures; the financial sector has put in place in order to control cybercrimes.

4.3 THE ZAMBIAN POLICE SERVICE[80]

The Zambian Police Service has put quite a number of measures in place to try and combat the rising and seemingly complicated crime. Among the measures the Service has outlined are the following:-

[80] The authority for the data on the measures being taken by the Zambia Police is Mr. Mukuka Chileshe, refer to note 59.

4.2.1 Media Awareness

The Police Service is undertaking some vigorous awareness campaigns. They are carrying out some Television educative talks to inform the public of the dangers and possibly how they can safeguard their information on the computers and phones.

4.2.2 Dialogue with the Banks

Another measure is that the Police Services is holding talks with the Banks who happen to be the major users of computers on the importance of ensuring total protection of their clients' information and monies that people deposit with them.

4.2.3 Educating Police Officers

Considering the rising of these crimes in Zambia, the Police Service has seen the need to educate the Police Officers on these crimes and how to investigate these sophisticated crimes because these are not just ordinary criminal offences. A lot more needs to be done in order to bring to book as cyber criminal as opposed to the ordinary cases.

4.2.4 Liaising with ZICTA

The Police Service is also working in corroboration with ZICTA who have the capacity in terms of technical know-how to deal with these cases. Most police officers are in fact computer illiterate and even the few who are able to use computers are not capable of investigating these crimes because it requires training in order for one to be able to bring out evidence against a criminal for example.

4.4 INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) SECTOR[81]

The Information and Communication Technology (ICT) Sector in Zambia which comprises among others the Zambia Information and Communications Technology Authority (ZICTA), The Computer Society of Zambia (CSZ), The Internet Service Providers (Zamnet, Iconnet, Uunet, Zamtel, Microlink, Real Time, Necor), The Mobile Service Providers (Zamtel, Airtel and MTN) to mention but a few have come up with some measures to curb cybercrimes. Some of these measures include the following:-

4.4.1 Collaboration among all stakeholders

It is not possible for one single organization to effectively fight cyber crimes because of the complicated nature of these crimes, therefore there should be serious collaborative efforts among various stakeholders in order to manage cyber cases. Some companies maybe skilled in certain areas of ICT while others are skilled in other areas of ICT altogether. These differences imply that without serious collaborations, cybercrimes will not be effectively fought. The ICT Sector is working with stakeholders like the Zambia Police Service in order for the Police Service to effectively tap in the wealth of cyber experts who can add value to computer forensic investigations and siphoning of digital evidence from computer various media.

4.4.2 Creation of a Data base of Cyber Criminals

The ICT Sector is also planning to create a database of cyber criminals so that once someone is entered into the database, he or she will not be offered a job in the sector until after some time.

4.4.3 Creating Public Awareness

The Sector through the Computer Society of Zambia has embarked on sensitization campaigns to educate the public through Television and Radio programs on the need to take security measures

[81] The authority for the information on the ICT Sector is **Mr. Emmanuel Chimuka**, an IT Manager at ZISC and also the Chairman for Midlands in the Computer Society of Zambia; (Interviewed on 28/12/ 2010)

as they go on doing their day to day work on the computers. This measure is already being implemented as some programs both on Television (ZNBC and Muvi) and on Radio 2 have already been aired. The Sector is also intending to carry out organizational workshops/seminars targeting at government departments, companies and other institutions, including individuals of the threat posed by cyber crimes in Zambia.

4.4.4 Capacity building for ICT Professionals

Organizations have a key responsibility to ensure that their ICT Professionals are well empowered with IT security skills in order to safeguard data/information resources. Investment in local IT Professionals is critically essential because it ensures internal responsibility and system ownership. It is a tremendously high risk to involve external IT experts on company systems as these external IT experts are capable of tempering with the system even when they are in their countries. In light of this, the Computer Society of Zambia plans to conduct seminars for ICT Professionals from various companies, the government and anyone who would be willing to learn the security skills.

From the foregoing, it is clear that the relevant stakeholders in regard to cybercrimes in Zambia are taking all the reasonable steps possible to try and minimize the commission of these crimes because eradicating them completely is not possible as history has shown that crime has always existed side by side with man.

CHAPTER FIVE

5.0 CONCLUSION/RECOMMENDATION

5.1 CONCLUSION

Cybercrime is a persisting international evil that transcends national boundaries in a manner that renders this form of organized crime a global concern. This fact can be substantiated by the July, 2010 debit card fraud on ATMs when cards were cloned and used in other countries[82] among other incidences that have been reported in this paper. Improving cyber security is therefore a global problem and each country in the region must improve its national efforts and undertake actions to join and support regional and international efforts to improve cyber security. Cybercrime may take several forms including online fraud, theft and cyber terrorism. It has been seen that amongst the major reasons that facilitate the perpetration of this crime is the globalization of technology and the revolutionary advancement of ICTs that have impacted on criminal activity.

Generally speaking, though these crimes are traceable, Zambia is still a safe haven. This can be seen from the few cases that have been prosecuted on the subject. It was difficult to believe that there was no case record in cybercrimes at the High Court. The prevalence rate is rather low and this is mainly because the crimes are not being reported partly due to the illiteracy levels with regard to computer usage. The expression of ignorance exhibited by some of the officers in some of the institutions visited during research was surprising. It would be beneficial in this regard for key officers in law enforcement agencies (Courts and the Police) especially to be equipped with the basic knowledge of and essential skills in ICTs in order for them to be fully functional and to render their services effectively and with confidence so as to be of help to the modern society which they service.

[82] Statement issued by Mr. Luke Njovu - Head of Corporate Affairs - Standard Chartered Bank: The Post, 29 July 2010

The battle against all forms of cybercrime requires immediate attention from all relevant actors in the cybercrime ecosystem, including the ICT regulators, and close collaboration and coordination among relevant parties and in some cases States. Analysis shows that innovative approaches to fighting cybercrime adopted by the ICT regulators can have a positive impact on end users' trust and confidence, which underpins the development of today's digital society and economy. Given the potential implications of cybercrime and threats to cyber security for the uptake of ICT services by citizens, businesses, and governments in developing countries, ICT regulators can be a key stakeholder in developing and implementing national strategies to respond to cybercrime.

As computers and the internet use increases, cyber incidents will also increase. The use of ICT's in the country is expected to increase exponentially in all sectors for example in e-Government, e-Banking, e-commerce, e- Learning, hence the need to protect infrastructure and data. We have a better chance to mitigate the effects of cybercrimes as a country if we create and sustain a co-ordinated, trustful alliance that the end users can depend on because the capacity of human mind is unfathomable. There is no limit to the way a human mind can think but it is in our hands to take precautions to prevent falling prey to such insidious acts. It is not possible to eliminate cybercrime from the cyberspace completely, it is quite possible though to check them as history is the witness to the fact that no legislation has succeeded in totally eliminating crime from the globe. The only possible step is to make people aware of their rights and duties (to report crime as a collective duty towards society) and further making the application of the laws more stringent to check crime and punish the few that are caught very severely.

5.2 RECOMMENDATIONS

Having labored to show the extent of cybercrimes in Zambia and the measures generally being taken or proposed to be undertaken by the various stakeholders in the ICT world, the following is hereby recommended:-

5.1.1 Members of the public should be aware of the need for security of information systems and networks

More still requires to be done besides what the various stakeholders are already doing because awareness of the risks and available safeguards is the first line of defence for the security of information systems and networks. Information systems and networks can be affected by both internal and external risks. Users should understand that security failures may significantly harm systems and networks under their control. They should also be aware of the potential harm to others arising from interconnectivity and interdependency. Members of the public should be aware of the configuration of, and available updates for their system, its place within networks, good practices that they can implement to enhance security, and the needs of other users.

5.1.2 Creation of a Computer Forensic Laboratory

Computer forensics is a branch of digital forensic science pertaining to legal evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of preserving, recovering, analyzing and presenting facts and opinions about the information. Although it is most often associated with the investigation of a wide variety of computer crime, computer forensics may also be used in civil proceedings. Evidence from computer forensics investigations is usually subjected to the same guidelines and practices of other digital evidence. A Computer Forensic Laboratory is a special lab that carries out critical investigations to bring about evidence for cybercrimes committed. As can be seen from this paper, cybercrimes in Zambian are on the increase hence the need for the government to consider opening up a forensic laboratory. The creation of a cyber forensic laboratory will help fight cybercrimes, investigations will be carried out expeditiously in order to bring out evidence, thus unearthing perpetrators of these crimes which in the end will act as a deterrent to offenders.

5.1.3 Child Pornography should be prohibited

Selling child Pornography materials to under age children should be prohibited by putting up stiffer laws in place and offenders should be given stiffer punishments. Children should not be allowed to access pornographic materials through computer media.

5.1.4 Organizations should be held responsible for the security of information systems and networks

All companies depend upon interconnected local and global information systems and networks and should understand their responsibility for the security of those information systems and networks. They should be accountable in a manner appropriate to their individual clients. Those who develop, design and supply products and services should address system and network security and distribute appropriate information including updates in a timely manner so that users are better able to understand the security functionality of products and services and their responsibilities related to security.

5.1.5 ICT Professionals should act in a timely and co-operative manner to prevent, detect and respond to security incidents

Recognizing the interconnectivity of information systems and networks and the potential for rapid and widespread damage, IT Professionals should act in a timely and co-operative manner to address security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective co-operation to prevent, detect and respond to security incidents. Where permissible, this may involve cross-border information sharing and co-operation since cybercrimes are committable across borders.

5.1.6 Computer users should respect the legitimate interests of others

Given the pervasiveness of information systems and networks in our societies, users need to recognize that their action or inaction may harm others. Ethical conduct is therefore crucial and participants should strive to develop and adopt best practices and to promote conduct that recognizes security needs and respects the legitimate interests of other users.

5.1.7 Companies should conduct risk assessments

Risk assessment identifies threats and vulnerabilities and should be sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications. Risk assessment will allow determination of the acceptable level of risk and assist the selection of appropriate controls to manage the risk of potential harm to information systems and networks in light of the nature and importance of the information to be protected. Because of the growing interconnectivity of information systems, risk assessment should include consideration of the potential harm that may originate from others or be caused to other users.

5.1.8 Companies should incorporate security as an essential element of information systems and networks

Systems, networks and policies need to be properly designed, implemented and coordinated to optimize security. A major, but by no means exclusive, focus of this effort is the design and adoption of appropriate safeguards and solutions to avoid or limit potential harm from identified threats and vulnerabilities. Both technical and non-technical safeguards and solutions are required and should be proportionate to the value of the information on the organization's systems and networks. Security should be a fundamental element of all products, services, systems and networks, and an integral part of system design and architecture.

5.1.9 Enactment of Legislation to Regulate the ICT Profession

Cyber criminals are generally considered to be Information Communication Technology professionals who are somehow disgruntled and want to vent their frustration on former employers. One of the best ways by which the government can effectively fight cyber crimes is to use the legal framework. Through enacting legislation that would regulate the conduct of professionals, government can achieve great strides in fighting cyber crimes. There is need for legislation which will regulate ICT Professionals in such a manner that if someone

commits a crime they should not only be punished by the courts of law but also be blackmailed and then finally deregistered from membership of the professional body which will make it difficult for such a person to easily get a job in another company.

Currently, the ICT Professionals are free to belong to the Computer Society of Zambia or not. It is purely voluntary. The implication is that cyber criminals would definitely not register for fear of adhering to the ICT code of conduct thus affecting their clandestine activities. These criminals would commit a crime in one organization and after a few months get another job in another organization which could be avoided if there were regulations in place.

BIBLIOGRAPHY

BOOKS

1. Fadia A, An Ethical Hacking Guide to Corporate Security, Macmillan India Ltd: Delhi (2006)

2. Scambray J., Liu V., Sima C., Hacking Exposed Web Applications: Web Application Security Secrets and Solutions, 3rd Ed., Tata McGraw Hill Education Private Ltd: New Delhi (2011)

OTHER WORKS REFERRED TO

1. Cell Phones - Hackers Next Target: MobileIN.com Home Page, (2009)

2. Denning, D.E., Cyber terrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services, U.S. House of Representatives, (2004)

3. Dick Johnston: Abstracts for Cyber Crime Summit: A Unique Challenge Requiring An Innovative Response

4. Goodman M.D. and Brenner S., The Emerging Consensus on Criminal Conduct in Cyberspace; Oxford, International Journal of Law and Information Technology, Vol.10, (2000)

5. Grabosky P. and Russell Smith, Sydney; Crime in the Digital Age: Federation Press, (1998) (co-published with the Australian Institute of Criminology)

6. Haines Howard; Cybercrime Law Separating Myth from Reality, (2010)

7. Johnson D. and Post D., Law and Borders: The Rise of Law in Cyberspace (Stanford, Stanford Law Review), (1996)

8. Kaplan Karen, Germany Forces Online Service to Censor Internet, L.A. Times, (1995)

9. Kapumba N. Doris, Obligatory Essay entitled: The Computer Misuse and Crimes Act of 2004: Its effectiveness in combating cyber crimes in Zambia, (2006)

10. Kevin G., Coleman of Technolytics ; Cyber Crime Mobile: (2009)

11. Krenz M., Cyber Crime - A New Way to Commit Old Crimes, (2004)

12. Kunz Michael & Patrick Wilson, Computer Crime and Computer Fraud; University of Maryland, Department of Criminology and Criminal Justice (2004)

13. Lim-Robrigado S., Poetic Justice: Cybercrimes, Electronic Money Laundering and Tax Evasion, (2009)

14. Ling Wai Chyuan; The importance of ICT for development, (2008)

15. Longe, F. A., The Design of An Information-Society Based Model For the Analysis of Risks and Stresses Associated Risks Associated with Information Technology Applications: Unpublished M. Tech. Thesis, FUT, Akure, Nigeria (2004)

16. Main K., eHow Contributor: (2010)

17. Mann and Sutton; Net crime: More change in the Organization of Thieving. British Journal of Criminology; 38: 201-229. Oxfordjournals.org; (1998)

18. Mefford, Lex Informatica: Foundations of the Law on the Internet (IJGLS), (1997)

19. Michael A. Sussmann, The Critical Challenges From the International High-Tech and Computer-Related Crime at the Millennium, 9 DUKE J. COMP. & INT'L L. 451, (1999)

20. Mohamed Chawki; A Critical Look at the Regulation of Cybercrime: A Comparative Analysis with Suggestions for Legal Policy; LL.B (1998)

21. Moore, R."Cybercrime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing (2005)

22. National Information and Communication Technology Policy; Ministry of Communications and Transport (April, 2006)

23. Olzak T., The five phases of a successful network penetration, (2008) http://www.techrepublic.com/blog/security/the-five-phases-of-a-successful-network-penetration/701

24. Ophardt, Jonathan A. "Cyber warfare and the crime of aggression: the need for individual accountability on tomorrow's battlefield" Duke Law and Technology Review, (2010)

25. Parker D., Computer Crime: For Protecting Fighting Information (U.S.A, John Wiley), (1998)

26. Rassolov I. Law and Internet – M., (2003)

27. Reed C., Computer Law (U.K, John Angel), (2004)

28. Sally Burnheim, "The Right to Communicate: The Internet in Africa," Article 19; Sub-Saharan Africa, (2006-2007)

29. Shinder D., Scene of the Cybercrime (U.S.A, Syngress), (2002)

30. Spinello R., Regulating Cyberspace: The Policies and Technologies of Control (U.S.A, Spinello), (2002)

31. Stocks B., Why Do People Commit Computer Crimes: (2009) (http://www.ehow.com/about)

32. United States. "Stalking and Domestic Violence Report to Congress" (2001)

33. Zittrain Jonathan, Charles Nesson and Lawrence Lessig: Internet Law: Foundation Press

WEBSITES VISITED FOR RESEARCH

1. www.unapcict.org/ecohub/resources/browse.../asean.../ict4d.../file
2. http://hubpages.com/hub/Cyber-Crime-The-Risk-Danger-and-Trends
3. http://www.techrepublic.com/blog/security/the-five- phases-of-a-successful-network-penetration/701
4. http://www.crime-research.org/library/Nomokonov.html
5. http://bjc.oxfordjournals.org/content/38/2/201.short
6. http://www.law.duke.edu/journals/dltr/articles/pdf/2010dltr003.pdf
7. http://www.ehow.com/about_4709031_do-people-commit-computer-crimes.html
8. http://ezinearticles.com/?expert=Mary_Krenz
9. http://www.spamlaws.com/types-of-cyber-crime.html
10. http://www.cs.georgetown .edu/~denning/infosec/cyberterror.htm
11. http://www.ehow.com/list_6307677_examples-cyber-crime.html
12. http://sheryl-lim-robrigado.blogspot.com/2009/11/cyber-crimes.html