

FOR USE IN THE LIBRARY ONLY

UNIVERSITY OF NAIROBI

FACULTY OF ARTS

DEPARTMENT OF POLITICAL SCIENCE AND PUBLIC
ADMINISTRATION

**CYBERCRIME IN KENYA:
MYTH OR REALITY**

UNIVERSITY OF NAIROBI
EAST AFRICANA COLLECTION

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILMENT OF
THE REQUIREMENTS FOR THE AWARD OF POST GRADUATE
DIPLOMA (PGD) IN STRATEGIC AND SECURITY STUDIES

BY: CHEBIEGON KANGOGO

C40/P/8202/06

University of NAIROBI Library



0444385 9

SUPERVISOR: MR. NIXON MUGANDA

16TH NOVEMBER 2008

DECLARATION


This research project is my own original work and has not been presented for any academic award in any institution of higher learning.

Signature  Date 2ND DEC. 2008

Chebiegon Kangogo

C40/P/8202/06

This research project has been submitted for examination with my approval as the University supervisor.

Signature  Date 6/12/2008

Mr. Nixon Muganda

University of Nairobi

DEDICATION

To all ICT professionals whose life's work is dedicated to ensuring security of our electronic communication.

ACKNOWLEDGEMENT

I would like to thank God for seeing me through the course and to the Government of Kenya for the scholarship to pursue a Post Graduate Diploma in Strategic and Security Studies. I thank Mr. Nixon Muganda for his scholarly advice and supervision. Special thanks to all the people who responded to my questionnaire for their invaluable input in my research. Thanks to my parents for their support and encouragement. Lastly, thanks to Adah for always having a second opinion.

ABSTRACT

There is a general feeling that Internet crime is an advanced type of crime that has not yet infiltrated developing countries like Kenya. The major assumption is that Cybercrime is silent and growing and that most Internet users have at one point fallen victim of Cybercrime. The victims suffer in silence, while the perpetrators continually hide under the invisibility of cyber space. The study was aimed at revealing the extent of the crime in Kenya and examined the levels, types, intensity and span of Cybercrime in Kenya.

The research questions addressed are; what types of Cybercrimes internet users in Kenya experience, what are the incidences of Cybercrime, what are the specific major cases of Cybercrime that have occurred in Kenya, is Kenya a target of cyber criminals and what measures can be put in place to curb Cybercrime in Kenya.

The data for this study was gathered through both primary and secondary sources. These included documented data and survey through questionnaires. The data analysis is both qualitative and quantitative.

The study found that cybercrime is indeed a major problem in Kenya. Though it is yet to manifest itself in Kenya to the proportions observed in the western world, it is worth noting that incidence of these is likely to go unreported due to lack of confidence in the law enforcers as shown by the research.

The conclusion of this study will form the basis of recommendations to ICT policy makers to realise the magnitude of Cybercrime and formulate policy to fight it, and also to Internet users and institutions on steps to take to avoid being victims of Cybercrime.

TABLE OF CONTENTS

1.0 INTRODUCTION.....	12
1.1 BACKGROUND OF THE STUDY.....	12
1.2 PROBLEM STATEMENT.....	15
1.3 OBJECTIVES OF THE STUDY.....	17
1.4 JUSTIFICATION OF THE STUDY.....	17
2.0 LITERATURE REVIEW.....	19
2.1 INTRODUCTION.....	19
2.2 VARIETY OF COMPUTER RELATED CRIMES.....	20
2.3 TOOLS AND TECHNIQUES OF CYBERCRIME.....	25
2.4 MOTIVATIONS AND OPPORTUNITIES FOR CYBERCRIME.....	27
2.5 THE CHALLENGE OF CONTROLLING COMPUTER-RELATED CRIME.....	29
2.6 CYBERCRIME ACTIVITIES IN KENYA.....	32
2.7 THE MAIN TYPES OF PC VIRUSES.....	34
2.8 EMAIL/INTERNET RELATED CRIMES.....	41
2.9 VULNERABILITY TO CYBER CRIMINALS.....	43
3.0 RESEARCH METHODOLOGY.....	47
3.1 INTRODUCTION.....	47
3.2 RESEARCH DESIGN.....	47
3.3 DESCRIPTION OF POPULATION.....	47
3.4 THE SAMPLE AND SAMPLING PROCEDURE.....	47
3.5 DESCRIPTION OF DATA COLLECTION TOOLS.....	48
3.6 DATA ANALYSIS PROCEDURES.....	49
4.0 RESEARCH FINDINGS AND ANALYSIS.....	51
4.1 INTRODUCTION.....	51
4.2 CYBERCRIME.....	51
4.3 BLACKMAIL EMAILS.....	52
4.4 SPAM.....	52

4.5	ELECTRONIC PIRACY	53
4.6	DENIAL OF SERVICE	54
4.7	SALES AND INVESTMENT FRAUD	55
4.8	TELEPHONE SERVICE THEFT	55
4.9	HACKING.....	56
4.10	EMAIL ATTACKS	56
4.11	VIRUSES, WORMS AND TROJANS.....	57
4.12	INTERNET TIME THEFT	58
4.13	LEVEL OF RISK OF CYBERCRIME.....	58
4.14	ELECTRONIC CARD THEFT.....	59
4.15	GOVERNMENT ACTION	60
5.0	RECOMMENDATIONS AND CONCLUSIONS	62
5.1	INTRODUCTION	62
5.2	THE CURRENT LEGAL SITUATION	63
5.3	THE EVIDENCE ACT.....	64
5.4	REGIONAL AND GLOBAL INVOLVEMENT.....	65
5.5	THE CHALLENGE	66
5.6	THE FUTURE OF CYBERCRIME	67
5.7	CHALLENGES FACING THE INTERNATIONAL COMMUNITY AND THE PRIVATE SECTOR	68
5.8	LIMITATIONS OF THE STUDY	69
5.9	RECOMMENDATION FOR FURTHER RESEARCH	70
	BIBLIOGRAPHY	71
	APPENDICES.....	73
	APPENDIX A: INTRODUCTORY STATEMENT	73
	APPENDIX B: QUESTIONNAIRE	74

TABLE OF FIGURES

Figure 1: Instances of cybercrime.....	51
Figure 2: Blackmail E-mail received.....	52
Figure 3: Unsolicited e-mails	53
Figure 4: Usage of Pirated Material.....	54
Figure 5: Denial of Service	54
Figure 6: Sales and Investment Fraud	55
Figure 7: Telephone service theft.....	55
Figure 8: Instances of hacking	56
Figure 9: E-mail attacks.....	57
Figure 10: Viruses, worms and trojans	Error! Bookmark not defined.
Figure 11: Internet time theft.....	58
Figure 12: Risk of cybercrime	59
Figure 13: Electronic card theft	59
Figure 14: Time taken to discover electronic card theft	60
Figure 15: Government action.....	60
Figure 16: Reporting cases of cybercrime	61

LIST OF ACRONYMS

ACRC	Advanced Computing Research Centre
APHIA	AIDS, Population, and Health Integrated Assistance Program
ATM	Automated Teller Machine
DNS	Domain Name System
DoS	Denial of Service
ICT	Information and Communications Technology
LAN	Local Area Network
MAC	Media Access Control
MANET	Mobile ad hoc networks
MBR	Master Boot Record
MTE	Mutation Engine
PEAP	Protected Extensive Authentication Protocol
PDA	Personal Digital Assistant
SSID	Service Set Identifiers
SNMP	Simple Network Management Protocol
TEMPEST	Transient Electromagnetic Pulse Emanation Standard
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WPA	WI FI Protected Access

DEFINITION OF TERMS

Cybercrime is a term used broadly to describe activity in which computers or networks are a tool, a target, or a place of criminal activity.

Media Access Control Address (MAC) is a unique code assigned to most forms of networking hardware. The address is permanently assigned to the hardware, thus limiting a wireless network's access to hardware – such as wireless cards – is a security feature employed by closed wireless networks.

Packet Sniffing is a technology used by crackers and forensics experts. This is when the offender is able to get unauthorised access to data by corrupting the information relay, which is in packets form within the network.

Password is a type of authentication. To crack a password means to decrypt a password, or to bypass a protection scheme.

Protected Extensive Authentication Protocol (PEAP) is a method used to securely transmit authentication information.

Service Set Identifiers (SSID) is software set by a network administrator and for open wireless networks. It is used to broadcast to all wireless devices within a range of the network access point.

Simple Network Management Protocol (SNMP) is a set of standards for communication with devices connected to a TCP/IP network. Examples of these devices include routers, hubs, and switches. A device is said to be 'SNMP compatible' if it can be monitored and/or controlled using SNMP messages.

Tempest is the ability to monitor electromagnetic emissions from computers in order to reconstruct the data. This allows remote monitoring of network cables or remotely viewing monitors.

Unauthorised Access is gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network.

Virtual Private Network (VPN) is a network that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable a user to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorised users can access the network and that the data cannot be intercepted.

1.0 INTRODUCTION

1.1 BACKGROUND OF THE STUDY

Cybercrime is a term used broadly to describe activity in which computers or networks are a tool, a target, or a place of criminal activity. Although the term cybercrime is usually restricted to describing criminal activity in which the computer or network is an essential part of the crime, this term is also used to include traditional crimes in which computers or networks are used to enable the illicit activity (Forde & Patterson, 2003).

The Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (Vienna, 10-17 April 2000) categorized five offenses as cyber-crime: unauthorized access, damage to computer data or programs, sabotage to hinder the functioning of a computer system or network, unauthorized interception of data to, from and within a system or network, and computer espionage (Forde & Patterson, 2003).

Another way to define cybercrime is simply as criminal activity involving the information technology infrastructure, including illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system). Data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (ID theft), and electronic fraud (Grabosky, 1998).

Cybercrime consists of specific crimes dealing with computers and networks (such as hacking) and the facilitation of traditional crime through the use of computers (child pornography, hate crimes, telemarketing /Internet fraud). In addition to Cybercrime, there is also "computer-supported crime" which covers the use of computers by criminals for communication and document or data storage. While these activities might not be illegal in and of themselves, they are often invaluable in the investigation of actual crimes. Computer technology presents many

new challenges to social policy regarding issues such as privacy, as it relates to data mining and criminal investigations (ibid).

There are two main aspects to Cybercrime. One involves the employment of the computers and their networks for unlawful purposes. Hacking is one such activity. This involves unauthorised electronic intrusion into a computer or a computer network for acquisition of important and confidential information. This information is then subjected to various forms of abuse, which may include theft of proprietary material. Business secrets are also abused and sensitive records manipulated while usernames, passwords and credit card numbers are acquired to facilitate fraud (ibid).

UNIVERSITY OF NAIROBI
EAST AFRICANA COLLECTION

A second example of this form of Cybercrime entails denial of service (or DoS) attacks. These occur when a saboteur deploys a computer - or a battery of them - to bombard a server hosting an important website with rapid streams of nonsense information. This causes the server in question to stall. The targeted website becomes unresponsive thus denying legitimate users of the service access to useful information or services. Often DoS attacks are directed against important service providers, such as search engines, news sites and e-mail hosts, common perpetrators being extortionists who hold the service provider at ransom.

The second aspect of the Cybercrime relates to utilisation of information technology as incidental aid to the actualisation of more conventional forms of crime. An example is the Nigerian fraud, which involved a 'confidential' e-mail, purportedly from a prominent Nigerian who wanted assistance to transfer ill-gotten funds offshore. Despite the patent dis-ingenuity of the pitch, the trick continued to net hundreds of victims every year.

Cybercrimes—harmful acts committed from or against a computer or network—differ from most terrestrial crimes in four ways. They are easy to learn how to commit; they require few resources relative to the potential damage caused; they can be committed in a jurisdiction without being physically present in it; and they are often not clearly illegal (Wahlert, 2002).

In the Kenyan context, perhaps the most evident variance between the law and Internet use centres on publication and consumption of prohibited material - pornography, to be specific. Despite the prohibition of trafficking, publishing and exhibition of obscene publications under section 181 of the Penal Code, the ready availability of sexually explicit material prevailed to the extent of causing public outcry on more than one occasion.

Of even greater concern is the use of the Internet as a conduit for illegal exploitation of intellectual property. A cursory study of any public cyber facility in Nairobi will reveal widespread popularity of what are commonly known as peer-to-peer networks - internet sites via which vast communities of net users freely swap pirated data, software, music and audio-visual material. The Kenyan government is however showing commitment in fighting cyber crime through enacting laws.

Kenya's cyber law, when enacted, could be adopted as a model law for other countries within the East African Community (EAC) — Tanzania, Uganda, Rwanda and Burundi — which are yet to enact such kind of legislation to give regulatory direction for ICT-related transactions (The Standard, 2007).

Already, a process has been initiated under the auspices of United States Agency for International Development (USAID) Washington's Economic Growth Agriculture and Trade/Information Technology and Energy (EGAT/IT&E) Bureau to guide the process leading to the development of the legislation in Kenya.

The initiative, called e-Legislation policy development initiative for the East African Community (EAC) — Kenya Cyber Law model, is facilitated through the Digital Opportunity through Technology and Communications Partnerships (DOT-COM), policy component that is managed by the Academy for Educational Development (AED).

The process is run in collaboration with Kenya's Directorate of e-Government and implemented by Afrika ICT Strategies Inc., a consulting and research firm with head offices in Washington, and a subsidiary office in Kenya (The Standard, 2007).

The initiative is in recognition of the fact that e-Transactions laws have the potential to generate significant economic and political development for Kenya and East Africa as a whole and this could attract criminals who would use loopholes to target computer users.

Moreover, the e-Transactions Bill will lay a strong foundation for the implementation of various e-Government and e-Commerce applications, including e-procurement, e-taxation, e-Land Registry, e-Funds Transfer among others.

Those involved in the e-Legislation policy development initiative for the East African Community (EAC) have recommended that the ministry of Information and Communication “considers replacing the Information Technology part of the KCA Bill, 2007, with a comprehensive e-Transactions Bill.” Such a Bill should build on various EAC and Kenya stakeholder forums. The Bill can be sponsored by the ministry of Information and Communication, Trade, Treasury or Tourism (The Standard, 2007).

1.2 PROBLEM STATEMENT

The current and anticipated changes in technology arising from the convergence of communications and computing are remarkable, and have already had a significant impact on many aspects of life. Banks, stock exchanges, air traffic control, telephones, electric power, and a wide range of institutions of health, welfare, and education are largely dependent on information technology and telecommunications for their operation.

The modern world is moving rapidly to the point where it is possible to assert that everything depends on computer software. The exponential growth of this technology, the increase in its capacity and accessibility, and the decrease in its cost, has brought about revolutionary changes in commerce, communications, entertainment, and crime, (Grant, David & Grabosky, 1997)

Along with this greater capacity, however, comes greater vulnerability. Information technology has begun to provide criminal opportunities to commit crime from their desks. The number of people with Internet connections continues to increase as the volume of electronic commerce in Kenya, and around the world increases and these not only does the increasing connectivity

increase the number of prospective victims of computer related crime, it also increases the number of prospective offenders, (Grabosky 2000).

The variety of criminal activity, which can be committed with or against information systems, is diverse. Some of these are not new in substance; only the medium is new. Others represent new forms of illegality altogether. The growing danger from crimes committed against computers, or against information on computers, is beginning to claim attention in national capitals. In most countries around the world, there exist laws that are likely to be unenforceable against such crimes. This lack of legal protection means that businesses and governments must rely solely on technical measures to protect themselves from those who would steal, deny access to, or destroy valuable information.

Though Cybercrime in Kenya is yet to manifest itself in the appalling proportions (as only less than 3% respondents surveyed by PWC have been targeted by cyber criminals) observed in the western world, it is worth noting that incidences of these is likely to go unreported due to lack of confidence in the law enforcers. There is also the tendency of corporate victims to cast a shroud of secrecy over attacks against them to avoid perceptions of ineptitude and diminished credibility, (Price Water House Coopers, 2004)

The current state of our legislation is dismally wanting as far as the protection of our collective and individual interests relating to the electronic domain are concerned. Save for section 2 of the Evidence Act (after amendment 69 of 2000), which makes a comprehensive definition of the word 'computer' for purposes of the act, our entire body of statute law remains entirely oblivious of the pervasive changes and developments produced by the digital era.

However, some electronic crimes inherently feature a non-electronic element that, by extension or analogy, places them within the scope of existing legislation. For instance, the most of common Internet swindles fall under section 313 of the Penal Code, which sanctions obtaining by false pretences. The same applies to the various forms of fraud, extortion and theft commonly perpetrated by electronic means. Similarly, there is also no doubt concerning

the proscriptive adequacy of existing laws on illegal distribution of copyrighted material, and publishing of libellous, seditious or obscene material (The Standard, 2007)

The problem, however, is not one of prohibition, but of enforcement. The nature of the World Wide Web and the ever-compounding complexity of electronic systems make the virtual arena difficult to administer, accordingly complicating the investigation and prosecution of Cybercrimes, a situation aggravated by the lack of a statutory structure to address these intricacies.

1.3 OBJECTIVES OF THE STUDY

The overall objective of this study is to assess whether the Cybercrimes in Kenya are a myth or reality. In order to realise this objective, the following objectives have been derived:

- To establish the types of Cybercrimes Internet users in Kenya experience.
- To establish the circumstances which facilitate Cybercrime in Kenya
- To find out the specific major cases of Cybercrime that has occurred in Kenya.
- To establish whether Kenya a target of cyber criminals

1.4 JUSTIFICATION OF THE STUDY

The results of this study will be informative to policy makers in the formation of legislation of Cybercrime laws. Actually, Kenyan laws have not catered for such crime as mentioned earlier apart from section 2 of the Evidence Act (after amendment 69 of 2000). Our entire body of statute law remains entirely oblivious of the pervasive changes and developments brought by the digital era. Hence, this study can be used as a benchmark or as a basis for formulating laws.

Academically, this study will be informative to academicians in the field of information technology, corporate business and criminology studies as it highlights trends and purpose of this kind of crime because this study is based on how, why, where and who is most likely to be a victim and or perpetrator. Professional bodies such as the Computer Society of Kenya will also benefit regarding recommendations this study has given in helping fight and protect Kenyans

from Cybercrime. Law enforcement institutions involved in the fight against Cybercrimes will benefit by better understanding the gravity of Cybercrime. This will help them in their continued fight against Cybercrime. To the Internet users and institutions, they will learn steps to take to avoid being victims of Cybercrime.

2.0 LITERATURE REVIEW

2.1 INTRODUCTION

This research focused on literature which is based on two aspects of Cybercrime as defined by (Hundley & Anderson, 2001) i.e. crimes committed using computers as instruments and crimes committed targeting computer systems. When the computer is used as an instrument of crime is where by criminals use computers to facilitate crime through the Internet methods to flash or pass encrypted messages around the globe. Another stance where the computer is used to facilitate crime is when fraud related crimes target electronic banking or electronic commerce. Computer programmes are manipulated to fraudulently use of Automated Teller Machine (ATM) cards and accounts, credit card frauds, which is frauds involving electronic funds transfers, telecommunication frauds and frauds relating to Electronic Commerce and Electronic Data Interchange, (Kumar, 2002).

Another category under Cybercrime that this research looks at is when the computer is a target of crime. Some of the crimes that would fall under this category are sabotage of computer systems or computer networks, sabotage of operating systems and programmes and theft of data/information. Other crimes under this category are the theft of intellectual property, such as computer software, theft of marketing information and blackmail based on information gained from computerized files, such as medical information, personal history, sexual preferences and financial data, (Kumar, 2002).

Similar to information and communications, technologies have provided a platform for social, business and political activity. They have also been readily adopted as a platform for other less pro-social activity. Such technology is a powerful tool for those committing crimes, by either attacking computers or using them to further other criminal activity. It is often said that there are no new crimes involving computers, rather, new ways of committing old crimes. To some extent that is true, but the digital age creates a completely new environment for criminal activity, (Krone, 2003).

Cybercrime is characterized by lack of standard definition of online crimes nationally or internationally. Due to differences in laws and policing, offenders are able to exploit these differences to commit crime. Another aspect of Cybercrime is that offenders are digitally networked and they use advanced computer skills, (Krone, 2003).

It is important to note that the behaviour and tools used by offenders online often have a legitimate use. Ordinary users are often unaware of illegal activity affecting them and may not know that an offender has hijacked their identity or computer. The move by criminals to specialise in various aspects of high tech crime is illustrated by the proliferation of malicious software, often developed by sophisticated hackers only to be taken up by less experienced users and launched onto the net infecting vulnerable machines.

Trojan Horse software is one such example that can be used to compromise machines by taking control of them over the Internet creating a 'bot army', which then can be hired out to spread spam, or commit a denial of service attack on another user. Hackers can steal credit card records or other identifying data, using them directly or selling them to commit identity fraud. Spam or directed attacks can also be used in phishing attacks to obtain access to finances online. The people needed to transfer the money back to the organisers of this sort of criminal activity can also be recruited online and then make their transactions online. All these products and services are now routinely networked among offenders enabling them to commit crimes. (ibid)

2.2 VARIETY OF COMPUTER RELATED CRIMES

The variety of criminal activity that can be committed with or against information systems is diverse. Some of these are not new in substance; only the medium is new. Others represent new forms of illegality altogether. The following generic forms of illegality involve information systems as instruments and/or as targets of crime.

2.2.1 Theft of Telephone Services

Telephone communication services theft is done by gaining access to an organisation's telephone switchboard (PBX). Individuals or criminal organisations can obtain access to dial-in/dial-out circuits and then make their own calls or sell call time to third parties, (Gold, 2004). Offenders may gain access to the switchboard by impersonating a technician, by fraudulently obtaining an employee's access code, or by using software available on the Internet. Some sophisticated offenders loop between PBX systems to evade detection. Additional forms of service theft include capturing "calling card" details and on-selling calls charged to the calling card account, and counterfeiting or illicit reprogramming of stored value telephone cards, (Schieck, 1995 and Newman, 1998). One significant case reported was that computer hackers in the United States illegally obtained access to Scotland Yard's telephone network and made £620,000 worth of international calls for which Scotland Yard was responsible, (Tendler and Nuttall 1996).

2.2.2 Use of cyber space for Criminal Conspiracies

Just as legitimate organisations in the private and public sectors rely upon information systems for communications and record keeping, so too are the activities of criminal organisations enhanced by technology.

Cyber space equipment is being used to facilitate organised drug trafficking, gambling, prostitution, money laundering, child pornography and trade in weapons (in those jurisdictions where such activities are illegal). The use of encryption technology may place criminal communications beyond the reach of law enforcement.

The use of computer networks to produce and distribute child pornography has become the subject of increasing attention. Today, these materials can be imported across national borders so fast, (Grant, David and Grabosky, 1997). By contrast, some of the less publicly visible traffic in child pornography activity appears to entail a greater degree of organisation. Although knowledge is confined to that conduct which has been the target of successful police investigation, there appear to have been a number of networks that extend cross-nationally,

use sophisticated technologies of concealment, and entail a significant degree of coordination, (Grabosky, 2000).

2.2.3 Electronic Piracy

Digital technology permits reproduction and easy dissemination of print, graphics, sound, and multimedia combinations. The temptation to reproduce copyrighted material for personal use, for sale at a lower price, or indeed, for free distribution, has proven irresistible to many.

This has caused considerable concern to owners of copyrighted material. Each year, it has been estimated that losses of between US\$15 and US\$17 billion are sustained by industry due to copyright infringement, (United States Information Infrastructure Task Force, 2000).

The Software Publishers Association has estimated that \$7.4 billion worth of software was lost to piracy in 1993 with \$2 billion of that being stolen from the Internet, (Meyer and Underwood, 2004).

The software industry plays a leading role in creating products that have vastly improved lives and work environment. Unfortunately, software theft, or piracy, has had a negative impact on the global marketplace and the ability to create new products. Copying in the workplace, counterfeiting and various forms of illegal distribution costs nearly \$12 billion each year, furthermore, the unauthorized electronic distribution and sale of copyrighted works over the Internet threatens to make these problems seem almost quaint by comparison, (Meyer and Underwood, 2004).

2.2.4 Dissemination of Offensive Materials

The rapid development of sophisticated and affordable computers and the increased accessibility of global telecommunications networks has revolutionised the manner in which information is transferred around the world. While the benefits of the global information exchange are enormous, attention has been drawn to the dangers of the free flow of certain material that has traditionally been the subject of control by law enforcement and customs authorities

Content considered by some to be objectionable exists in abundance in cyberspace. This includes, among much else, sexually explicit materials, racist propaganda, and instructions for the fabrication of incendiary and explosive devices. Computer systems can also be used for harassing, threatening or intrusive communications, from the traditional obscene telephone call to its contemporary manifestation in "cyber-stalking", in which persistent messages are sent to an unwilling recipient, (Akdeniz, 1999)

Computer networks may also be used in furtherance of extortion. The Sunday Times (London) reported in 1996 that over 40 financial institutions in Britain and the United States had been attacked electronically over the previous three years. In England, financial institutions were reported to have paid significant amounts to sophisticated computer criminals who threatened to wipe out computer systems, (The Sunday Times, June 2, 1996). The article cited four incidents between 1993 and 1995 in which a total of 42.5 million Pounds Sterling were paid by senior executives of the organisations concerned, who were convinced of the extortionists' capacity to crash their computer systems, (Denning, 1999).

UNIVERSITY OF NAIROBI
EAST AFRICANA COLLECTION

2.2.5 Electronic Vandalism, Terrorism and Extortion

The industrial society is dependent upon complex data processing and telecommunications systems. Damage to, or interference with, any of these systems can lead to catastrophic consequences. Whether motivated by curiosity or malice, electronic intruders cause inconvenience and have the potential for inflicting massive harm, (Hundley and Anderson, 2000).

While this potential has yet to be realised, a number of individuals and protest groups have hacked the official web pages of various governmental and commercial organisations, (Rathmell, 1997). This may also operate in reverse: early in 1999, an organised hacking incident was apparently directed at a server that hosted the Internet domain for East Timor, (Creed, 1999). An extortionist in Eastern Europe obtained the credit card details of customers of a North American based on-line music retailer, and published some on the Internet when the retailer refused to comply with his demands, (Markoff, 2000).

Cyber-terrorism is distinguished from other acts of commercial crime or incidents of hacking by its severity. Attacks against computer networks or the information stored there in which result in "violence against persons or property, or at least cause enough harm to generate fear" are to be considered cyber-terrorism attacks according to congressional testimony from Georgetown University professor Dorothy Denning. "Attacks that disrupt nonessential services or that are mainly a costly nuisance" are not classified as cyber-terrorist attacks by her definition, (Grabosky, 2000)

2.2.6 Sales and Investment Fraud

As electronic commerce becomes more prevalent, the application of digital technology to fraudulent endeavours will be greater. The use of the telephone for fraudulent sales pitches, deceptive charitable solicitations, or bogus investment overtures is increasingly common. Cyberspace now abounds with a wide variety of investment opportunities, from traditional securities such as stocks and bonds, to more exotic opportunities, the sale and leaseback of automatic teller machines, and worldwide telephone lotteries, (Cella and Stark, 1997). The digital age has been accompanied by unprecedented opportunities for misinformation. Fraudsters now enjoy direct access to millions of prospective victims around the world, instantaneously and at minimal cost, (Cella and Stark, 1997).

2.2.7 Electronic Funds Transfer Fraud

Electronic funds transfer systems have begun to proliferate, and so has the risk that such transactions may be intercepted and diverted. Valid credit card numbers can be intercepted electronically, as well as physically; the digital information stored on a card can be counterfeited.

In 1994, 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. Although Russian law precluded Levin's extradition, he was arrested during a visit to the United States and subsequently imprisoned, (Denning, 1999).

2.2.8 Electronic Card Theft

Credit card fraud is a wide-ranging term for theft and fraud committed using a credit card or any similar payment mechanism as a fraudulent source of funds in a transaction. The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account. Credit card fraud is also an adjunct to identity theft

According to Visa International, Kenya is Visa's fastest growing market in Africa outside South Africa, with \$452 million processed through the Visa credit and Electron debit cards last year. Recent media reports indicated that electronic card fraud in Kenya stood at Ksh10 million (\$128,205) a month, and that it was putting off both potential users and outlet merchants (Muniata, 2004)

2.3 TOOLS AND TECHNIQUES OF CYBERCRIME

The main technique used by cyber criminals is unauthorized access. This means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network. (Grabosky & Smith, 1998) Unauthorised access therefore means any kind of access without the permission of either the rightful owner or the person in charge of a computer, computer system or computer network. Thus not only would accessing a server by cracking its password authentication system be unauthorised access, switching on a computer system without the permission of the person in charge of such a computer system would also be unauthorised access. Packet sniffing, tempest attack, password cracking and buffer overflow are common techniques used in Cybercrime, (Awana, 2006).

2.3.1 Packet Sniffing

Packet Sniffing is a technology used by crackers and forensics experts alike. This is when the offender is able to get unauthorised access to data by corrupting the information relay, which is in packets form within the network. When the packets have been intercepted, then an adversary (a person trying to hack into a system) translates them back from encryption to the actual data. For doing this, he would normally use a technology called "Packet Sniffing". When he uses this technology, he is able to intercept all or some of the packets leaving the victim (sender) computer. The same deception can also be practiced at the point of the intended recipient of the message before it can actually receive the packets, (Awana, 2006).

2.3.2 Tempest attack

Tempest is the ability to monitor electromagnetic emissions from computers in order to reconstruct the data. This allows remote monitoring of network cables or remotely viewing monitors. The word TEMPEST is usually understood to stand for "Transient Electromagnetic Pulse Emanation Standard". Some fonts remove the high-frequency information, and thus severely reduce the ability to text on the screen. PGP also provides this option of using tempest resistant fonts. An appropriately equipped car can park near the target premises and remotely pick up all the keystrokes and messages displayed on the computer video screen. This would compromise all the passwords, messages, and so on. This attack can be thwarted by properly shielding computer equipment and network cabling so that they do not emit these signals, (Awana, 2006).

2.3.3 Password cracking

A password is a type of authentication. To crack a password means to decrypt a password, or to bypass a protection scheme. When the UNIX operating system was first developed, passwords were stored in the file "/etc/passwd". This file was readable by everyone, but the passwords were encrypted so that a user could not figure out what a person's password was. The passwords were encrypted in such a manner that a person could test a password to see if it was valid, but could not decrypt the entry. However, a program called "crack" was developed that

would simply test all the words in the dictionary against the passwords in "/etc/passwd". This would find all user accounts whose passwords were chosen from the dictionary. Typical dictionaries also included people's names since a common practice is to choose a spouse or child's name (Awana, 2006).

The "crack" program is a useful tool for system administrators. By running the program on their own systems, they can quickly find users who have chosen weak passwords. In other words, it is a policy enforcement tool. Password crackers are utilities that try to 'guess' passwords. One way, also known as a dictionary attack involves trying out all the words contained in a predefined dictionary of words. Ready-made dictionaries of millions of commonly used passwords can be freely downloaded from the Internet, (Awana, 2006).

2.3.4 Buffer overflow

Also known as buffer overrun, input overflow and unchecked buffer overflow. This is probably the most common way of breaking into a computer. It involves input of excessive data into a computer. The excess data "overflows" into other areas of the computer's memory. This allows the hacker to insert executable code along with the input, thus enabling the hacker to break into the computer, (Awana, 2006).

2.4 MOTIVATIONS AND OPPORTUNITIES FOR CYBERCRIME

To better prevent, detect and deal with cybercrimes, one might strive to understand the profiles and the motivations of cybercriminals. Understanding a hacker's motivation and level of technical skills can help to assess how serious an attack is, and assist in devising a counter-strategy. In order to secure an information system, one also needs to know the opportunities that cybercriminals exploit to attack their victims.

2.4.1 The drive behind Cybercrime

Computer-related crime, like crime in general, may be explained by the conjunction of three factors: motivation, opportunity, and the absence of capable guardianship. Motivations would vary depending on the nature of the crime in question, but may include greed, lust, revenge, challenge or adventure. Opportunities are expanding dramatically with the rapid proliferation and penetration of digital technology and significant challenges are posed by the transnational nature of much computer crime. The most appropriate strategies for the control of computer-related crime entailed a mixture of law enforcement, technological and market-based solutions. (Grabosky, 2000)

However, there is more to crime than opportunity. Crime requires a pool of motivated offenders, and a lack of what criminologists refer to as 'capable guardianship'; someone to keep watch. Much of computer-related illegality lies beyond the capacity of contemporary law enforcement and regulatory agencies alone to control, and that security in cyberspace depends on the efforts of a wide range of institutions, as well as on a degree of self-help by potential victims of cyber-crime, (ibid).

2.4.2 Motivations of computer criminals

The motivations of those who would commit computer related crime are diverse. Computer criminals are driven by time-honoured motivations, the most obvious of which are greed, lust, power, revenge, adventure, and the desire to push the limits. The ability to make an impact on large systems may, as an act of power, be gratifying in and of itself. The desire to inflict loss or damage on another may also spring from revenge, as when a disgruntled employee shuts down an employer's computer system, or to ideology, as when one defaces the web page of an institution that one regards as abhorrent. Much activity on the electronic frontier entails an element of adventure, the exploration of the unknown. The very fact that some activities in cyberspace are likely to elicit official condemnation is sufficient to attract the defiant, the rebellious, or the irresistibly curious. Given the degree of technical competence required to commit many computer-related crimes, there is one other motivational dimension worth

noting here. This, of course, is the intellectual challenge of mastering complex systems. None of the above motivations is new. The element of novelty resides in the unprecedented capacity of technology to facilitate acting on these motivations, (Denning, 2001).

2.4.3 Opportunities for computer-related crime

Recent and anticipated changes in technology arising from the convergence of communications and computing are remarkable, and have already had a significant impact on many aspects of life. Banking, stock exchanges, air traffic control, telephones, electric power, and a wide range of institutions of health, welfare, and education are largely dependent on information technology and telecommunications for their operation. The technology world is moving rapidly to the point where it is possible to assert, "Everything depends on software" (Grant, David \$ Grabosky, 1997). The exponential growth of this technology, the increase in its capacity and accessibility, and the decrease in its cost, has brought about revolutionary changes in commerce, communications, entertainment, and crime. Along with this greater capacity, however, comes greater vulnerability.

2.5 THE CHALLENGE OF CONTROLLING COMPUTER-RELATED CRIME

It is an immense challenge to control cybercrime, but for it to be done effectively then the motives and opportunities have to be addressed.

2.5.1 Motives

Crime can be explained in part by the supply of motivated offenders. Given the diversity of computer-related crime, it is not surprising that the various types of behaviour greed, lust, power, revenge, adventure, flow from a wide range of motives. Some of these include greed, lust, revenge and curiosity. Revenge in the modern era can also entail an ideological dimension. Of considerable significance, if not unique to computer-related crime, is the intellectual challenge of defeating a complex system. Motivations, whether on the part of individuals or in the aggregate, are very difficult to change. For this reason, the most strategically advantageous approaches to computer-related crime will be concerned with the reduction of opportunities, and with the enhancement of guardianship.

2.5.2 Opportunities

While motives tend not to change, the variety and number of opportunities for Cybercrime are proliferating. The exponential growth in connectivity of computing and communications creates parallel opportunities for prospective offenders, and parallel risks for prospective victims. As the Internet becomes increasingly a medium of commerce, it will become increasingly a medium of fraud.

The most effective way of eliminating opportunities for on-line crime is simply to pull the plug. This is of course unrealistic; most nations of the world are now highly dependent on information technology. For the poorer nations, information technology is probably a necessary, if not sufficient, path to economic development. Thus, the challenge lies in managing risk to achieve the maximum benefits, which flow from new technologies, while minimizing the drawback.

There are many technologies, which reduce the opportunity to commit computer-related crime. Given that so much computer-related crime depends upon unauthorised access to information systems, access control and authentication technologies have become essential. Sophisticated advice and products for computer crime prevention are provided by one of the world's growth industries of today, namely computer security.

Denning (1999) offers a comprehensive inventory of technologies for reducing opportunities for computer crime. She describes technologies of encryption and anonymity, which permit concealment of the content of communications such as a consumer's credit card details, or of the identity of the communicator, (not all participants in discussion groups on reproductive health wish to disclose their identities). Denning also outlines technologies of authentication, from basic passwords, to various biometric devices such as fingerprint or voice recognition technology, and retinal imaging, which greatly enhance the difficulty of obtaining unauthorised access to information systems.

Virus detectors can identify and block malicious computer code; blocking and filtering programs can screen out unwanted content. A rich variety of commercial software now exists with which to block access to certain sites, (Gold, 1993).

2.5.3 Guardians

The third basic factor, which explains computer related crimes, is the absence of a capable guardian. Capable guardianship has evolved over human history, from feudalism, to the rise of the state and the proliferation of public institutions of social control, to the post-modern era in which employees of private security services vastly outnumber sworn police officers in many industrial democracies.

Guardianship against conventional crime involves preventive efforts on the part of prospective victims, contributions by members of the general public or commercial third parties, as well as the activities of law enforcement agencies. Indeed, it is often only when private efforts at crime prevention fail that the criminal process is mobilised. So it is that owners of motor vehicles are encouraged to lock their vehicles at all times, that insurance contracts may offer premium discounts for crime prevention measures such as theft alarms, and that some car parks have video surveillance or private security guards in attendance. Often, it is only when these systems fail that the assistance of law enforcement is sought.

Technology can also enhance guardianship. Denning (1999) describes various technologies for detecting attempted intrusions of information systems. Alarms can indicate when repeated login attempts fail because of incorrect passwords, or when access is sought outside of normal working hours. Other anomaly detection devices will identify unusual patterns of system use, including atypical destination and duration of telephone calls, or unusual spending patterns using credit cards.

Guardianship can also be enhanced by market forces. A market is currently emerging for Internet service providers specializing in content suitable for family consumption, guaranteed to be free of sex, violence, and vilification.

Market forces may also generate second-order controlling influences. As large organisations begin to appreciate their vulnerability to electronic theft or vandalism, they may be expected to insure against potential losses. It is very much in the interests of insurance companies to require appropriate security precautions on the part of their policyholders. Indeed, decisions to set and to price insurance may well depend upon security practices of prospective policyholders.

2.6 CYBERCRIME ACTIVITIES IN KENYA

Kenya has had its fair share of Cybercrime ranging from virus attacks, identity theft, e-mail attacks, and software piracy. Among those, which have been reported, include the notice by the Nakumatt Supermarkets in its website. The notice was to warn its customers (smart card holders) that there were some deceitful operators, masquerading as Nakumatt officials, roaming around with the intent of obtaining bank details from them. Once these details were acquired, various cyber criminal activities can be conducted. Identity theft is one of the most nefarious, (Ngugi, 2006)

Identity theft occurs when a fraudster steals your name and other personal information for fraudulent purposes. It is a form of crime where somebody uses a false identity to commit a crime. This type of crime has been made considerably easier to commit due to the inherent loopholes that exist in ICT systems. The main documents used for harvesting identity details include birth certificates, bank statements, credit/debit card slips, driving licences, passports and land registry documents. These documents are all over. Someone can bribe a Posta employee to intercept your bank statements. Financial information can also be supplied to rings of fraudsters by corrupt bank staff. Cheques are a considerable risk. Banks have this habit of writing your account number, ID number and PIN number at the back. As a result, all your details are conveniently located in this document, (Ngugi, 2006).

Another case, which has been reported in Kenya, was the Equity Bank's website defacement. The cracker who defaced Equity's site might not have caused serious loss to the bank apart

from denting the reputations of the in-house IT team. However, this exposes a security lapse that would have had more implications that are serious. Such as the case of system intrusion of TJ-Maxx and its affiliates and during this incident, over 45.7 million payment card details, owned by customers of this firm, were stolen. The more startling aspect of it was that this data was accessed during an 18-month period from around July 2005 to December 2006. The breach was only made public in March 2007, (BBC, 2007).

Electronic theft in Kenya has also been reported. A gang of robbers broke into the Pastoral Centre Offices of the AIDS, Population, and Health Integrated Assistance Program (Aphia II) in Tudor, Mombasa. They broke into the main office and stole 20 computers, which were carted away in a vehicle. The greater loss, according to the report, was the vital data stored in the computers in favour of HIV/AIDS patients in the Coast Province, (Coastweek, 2007).

Wamuyu reports on that similar thefts have taken place in the ministry of office of the president, parastatal and corporate offices, especially in Nairobi. An office was burnt down maliciously to destroy electronic information, (ibid).

An article was carried out in the local newspaper detailing how Internet pornography has taken root in Kenya yet nothing has been done legally to prohibit this. The article details that dressed in full uniform, a policeman walks into a downtown cyber cafe to send an email and pretends not to see the site a 12-year-old boy is browsing, despite the bright coloured images on the computer screen. (Kwamboka, 2003)

The officer understands very well that public viewing of pornographic material is illegal in the country, but he is unable to arrest the boy or the owner of the cyber cafe because he cannot remember any law that directly addresses browsing such offensive sites at a private business. Pornography and obscenity is so rife on the Internet that any user is likely to run into erotic images or content while trying to open their e-mail accounts or while conducting a search online. Any mistyping or misspelling of a domain name can easily land a surfer onto a pornography site. The perverts are now capitalising on the gullibility of children, who are increasingly using the Internet as a way of exploring the world with the help of technology.

from denting the reputations of the in-house IT team. However, this exposes a security lapse that would have had more implications that are serious. Such as the case of system intrusion of TJ–Maxx and its affiliates and during this incident, over 45.7 million payment card details, owned by customers of this firm, were stolen. The more startling aspect of it was that this data was accessed during an 18-month period from around July 2005 to December 2006. The breach was only made public in March 2007, (BBC, 2007).

Electronic theft in Kenya has also been reported. A gang of robbers broke into the Pastoral Centre Offices of the AIDS, Population, and Health Integrated Assistance Program (Aphia II) in Tudor, Mombasa. They broke into the main office and stole 20 computers, which were carted away in a vehicle. The greater loss, according to the report, was the vital data stored in the computers in favour of HIV/AIDS patients in the Coast Province, (Coastweek, 2007).

Wamuyu reports on that similar thefts have taken place in the ministry of office of the president, parastatal and corporate offices, especially in Nairobi. An office was burnt down maliciously to destroy electronic information, (ibid).

An article was carried out in the local newspaper detailing how Internet pornography has taken root in Kenya yet nothing has been done legally to prohibit this. The article details that dressed in full uniform, a policeman walks into a downtown cyber cafe to send an email and pretends not to see the site a 12-year-old boy is browsing, despite the bright coloured images on the computer screen. (Kwamboka, 2003)

The officer understands very well that public viewing of pornographic material is illegal in the country, but he is unable to arrest the boy or the owner of the cyber cafe because he cannot remember any law that directly addresses browsing such offensive sites at a private business. Pornography and obscenity is so rife on the Internet that any user is likely to run into erotic images or content while trying to open their e-mail accounts or while conducting a search online. Any mistyping or misspelling of a domain name can easily land a surfer onto a pornography site. The perverts are now capitalising on the gullibility of children, who are increasingly using the Internet as a way of exploring the world with the help of technology.

They are also heedless and can easily reveal their personal details, including age, to strangers on the Internet. (Kwamboka, 2003)

Whenever children stumble upon a pornography site, this usually unlocks an avalanche of new pornography windows, making it an addictive vicious circle. As battle on pornography rages, the immoral material is readily available, with some cartels specialising on perverting young minds. Some cyber cafés operators and parents are now blocking some of the notorious pornography sites to protect children. Whenever one attempts to access these sites, a message appears on the screen warning that access cannot be allowed. (Kwamboka, 2003)

Virus attacks and email related crime are prominent in Kenya. A computer virus is a computer program that can infect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of it. Note that a program does not have to perform outright damage (such as deleting or corrupting files) in order to be called a "virus".

Many people use the term loosely to cover any sort of program that tries to hide its (malicious) function and tries to spread onto as many computers as possible. Viruses are very dangerous; they are spreading faster than they are being stopped, and even the least harmful of viruses could be fatal. For example, a virus that stops a computer and displays a message, in the context of a hospital life-support computer, could be fatal. Even the creator of a virus cannot stop it once it is spread out, (Awana, 2006).

2.7 THE MAIN TYPES OF PC VIRUSES

Generally, there are two main classes of viruses in Kenya and the wider web. The first class consists of the file infectors, which attach themselves to ordinary program files. These usually infect arbitrary .COM and/or .EXE programs, though some can infect any program for which execution is requested, such as .SYS, .OVL, .PRG, & .MNU files. File infectors can be either direct action or resident. A direct-action virus selects one or more other programs to infect each time the program that contains it is executed. A resident virus hides itself somewhere in memory the first time an infected program is executed, and thereafter infects other programs when they

are executed (as in the case of the Jerusalem 185 virus) or when certain other conditions are fulfilled. Most other viruses are resident. The second category is system or boot-record infectors: those viruses that infect executable code found in certain system areas on a disk, which are not ordinary files. On DOS systems, there are ordinary boot-sector viruses, which infect only the DOS boot sector, and MBR viruses that infect the Master Boot Record on fixed disks and the DOS boot sector on diskettes.

File system or cluster viruses (e.g. Dir-II) are those that modify directory table entries so that the virus is loaded and executed before the desired program is. Note that the program itself is not physically altered; only the directory entry is. Some consider these infectors to be a third category of viruses, while others consider them to be a sub-category of the file infectors, (Awana, 2006).

2.7.1 Stealth virus

A stealth virus is one that hides the modifications it has made in the file or boot record usually by monitoring the system functions used by programs to read files or physical blocks from storage media, and forging the results of such system functions so that programs which try to read these areas see the original uninfected form of the file instead of the actual infected form. Thus, the viral modifications go undetected by anti-viral programs. However, in order to do this, the virus must be resident in memory when the anti-viral program is executed, (Patel, 2003). The very first DOS virus, Brain, a boot-sector infector, monitors physical disk I/O and redirects any attempt to read a Brain-infected boot sector to the disk area where the original boot sector is stored. The next viruses to use this technique were the file infectors Number of the Beast and Frodo.

2.7.2 Polymorphic virus

A polymorphic virus is one that produces varied (yet fully operational) copies of itself, in the hope that virus scanners will not be able to detect all instances of the virus. The most sophisticated form of polymorphism discovered so far is the MtE "Mutation Engine" written by the Bulgarian virus writer who calls himself the "Dark Avenger", (Patel, 2003).

2.7.3 Fast and slow infectors

A typical file infector (such as the Jerusalem) copies itself to memory when a program infected by it is executed, and then infects other programs when they are executed. A fast infector is a virus which, when it is active in memory, infects not only programs which are executed, but also those which are merely opened. The result is that if such a virus is in memory, running a scanner or integrity checker can result in all (or at least many) programs becoming infected all at once.

The term "slow infector" is sometimes used for a virus that, if it is active in memory, infects only files as they are modified (or created). The purpose is to fool people who use integrity checkers into thinking that the modification reported by the integrity checker is due solely to legitimate reasons. An example is the Darth Vader virus, (Awana, 2006).

UNIVERSITY OF NAIROBI
EAST AFRICANA COLLECTION

2.7.4 Sparse infector

The term "sparse infector" is sometimes given to a virus that infects only occasionally, e.g. every 10th executed file, or only files whose lengths fall within a narrow range, etc. By infecting less often, such viruses try to minimize the probability of being discovered by the user.

2.7.5 Companion virus

A companion virus is one that, instead of modifying an existing file, creates a new program, which (unknown to the user) is executed by the command-line interpreter instead of the intended program. (On exit, the new program executes the original program so things will appear normal.) This is done by creating an infected .COM file with the same name as an existing .EXE file. Note that this type of malicious code is not always considered a virus, since it does not modify existing files, (Patel, 2003).

2.7.6 Armoured virus

An armoured virus is one that uses special tricks to make the tracing, disassembling and understanding of its code more difficult. A good example is the Whale virus.

2.7.7 Macro virus

Many applications allow you to create macros. A macro is a series of commands to perform an application-specific task. Those commands can be stored as a series of keystrokes, or as a special macro language.

A macro virus is a virus that propagates through only one type of program, usually either Microsoft Word or Microsoft Excel. It can do this because these types of programs contain auto open macros, which automatically run when you open a document or a spreadsheet. Along with infecting auto open macros, the macro virus infects the global macro template, which is executed anytime you run the program. Thus, once your global macro template is infected, any file you open after that becomes infected and the virus spreads.

2.7.8 Virus hoax

A virus hoax generally appears as an email message that describes a particular virus that does not exist. These emails usually carry the same basic story, that if you downloaded an email with a particular subject line, your hard drive will be erased (impossibility because the text of an email cannot harbour a virus).

Such messages are designed to panic computer users. The writer or writers email the warning and include a plea for the reader to forward it to others. The message then acts much like a chain letter, propagating throughout the internet as individuals receive it and then innocently forward it. An example of a virus hoax is the "Good Times" virus - which was written in 1994 and since then has circled the globe many times over. The best thing to do on receipt of such an email is to ignore and delete it. (Patel, 2003)

2.7.9 Worms

A computer worm is a self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems (usually via network connections). Unlike viruses, worms do not need to attach themselves to a host program. There are two types of worms - host computer worms and network worms.

2.7.7 Macro virus

Many applications allow you to create macros. A macro is a series of commands to perform an application-specific task. Those commands can be stored as a series of keystrokes, or in a special macro language.

A macro virus is a virus that propagates through only one type of program, usually either Microsoft Word or Microsoft Excel. It can do this because these types of programs contain auto open macros, which automatically run when you open a document or a spreadsheet. Along with infecting auto open macros, the macro virus infects the global macro template, which is executed anytime you run the program. Thus, once your global macro template is infected, any file you open after that becomes infected and the virus spreads.

2.7.8 Virus hoax

A virus hoax generally appears as an email message that describes a particular virus that does not exist. These emails usually carry the same basic story: that if you download an email with a particular subject line, your hard drive will be erased (impossibility because the text of an email cannot harbour a virus).

Such messages are designed to panic computer users. The writer or writers email the warning and include a plea for the reader to forward it to others. The message then acts much like a chain letter, propagating throughout the Internet as individuals receive it and then innocently forward it. An example of a virus hoax is the "Good Times" virus -- which was written in 1994 and since then has circled the globe many times over. The best thing to do on receipt of such an email is to ignore and delete it, (Patel, 2003).

2.7.9 Worms

A computer worm is a self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems (usually via network connections). Unlike viruses, worms do not need to attach themselves to a host program. There are two types of worms - host computer worms and network worms.

Host computer worms are entirely contained in the computer they run on and use network connections only to copy themselves to other computers. Host computer worms where the original terminates itself after launching a copy on another host.

Network worms consist of multiple parts (called "segments"), each running on different machines and using the network for several communication purposes. Propagating a segment from one machine to another is only one of those purposes, network worms that have one main segment, which coordinates the work of the other segments (Forde & Patterson, 2003).

The first worms in history were actually designed to good rather than harm to networks. The first ever programme that could be called a worm, as per definition, was developed for the assistance of air traffic controllers by Bob Thomas in 1971. This worm programme would notify air traffic controllers when the controls of a plane moved from one computer to another. In fact, this worm named "creeper" would travel from one computer screen to the other on the network showing the message, "I'm reeper! Catch me if you can!" The difference from most worms was that this creeper did not reproduce itself. Even later, although the idea of developing worms slowly faded away, a few people did try to experiment with these. These included John Shock and Jon Hepps of Xerox's Palo Alto Research Centre, who in the early 1980s began working on worm programmes. This was also the first time that this type of programme was called a worm (Grant, David & Grabosky, 1997).

Both of them developed a total of 5 worms, each specially designed to perform a particular function. They were programmed to do certain tasks around the network. The simplest of these worms was a "town crier" worm. Its job was only to post announcements on all the computers of the network. Then there were the more complicated worms, like the one, which would remain completely dormant during the day and would activate only in the night. Once all the employees had left for the day, this worm would harness the extra computing power of the idle computers to do tasks, which required more computing power. In the morning, before the arrival of the employees it would save all the work done during the night and become dormant until the next evening (ibid).

Although these programmes were apparently helpful around the network, their developers were given a rude glimpse of their inherent destructive possibilities when one morning the employees returned to find that all the computers had crashed. When they tried to restart the computers, they crashed again. It was found that one of the worms had malfunctioned and had created havoc in the network. A "vaccine" had to be created so as to deactivate the worm before the computers on the network could become functional again. The following are some of prominent types of worms (Grant, David & Grabosky, 1997).

On November the 22nd, 1988, Robert Morris, a Cornell University science graduate accidentally released his worm on a very large network in the area. This network was named Arpanet, which later went on to become the Internet. The worm managed to infect approximately three thousand computers during eight hours of activity. The Internet worm, as it came to be known, disabled all those machines by making copies of itself and thus clogging them. Apart from clogging all the security loopholes, many machines had to be completely taken off the network till all copies of the worm could be totally removed. Although the entire process took the scientists almost two to three days, no data was lost on any of the infected computers and no permanent damage was done to any of the computers (Lanham, Weinberg, Brown, & Ryan, 1997).

The Christmas tree worm, which was a combination of a Trojan Horse (a programme which does something more than what is entered in its specifications) and a chain letter. This was a mainframe worm and managed to paralyze the IBM network on Christmas day 1987. The worm was written in a language called Exec. It asked the user to type the word "Christmas" on the screen. Then it drew a Christmas tree and sent itself to all the names of people stored in the user files "Names" and "Netlog" and in this way propagating itself (ibid).

2.7.10 Trojans

This is a program a criminal uses to infect a computer user. Trojan horse program pretends to do one thing while actually doing something completely different in a computer.

Remote Administration Trojans (RATs) are the most popular Trojans. They let a hacker access the victim's hard disk, and perform many functions on his computer such as shutting down his computer, opening and closing his CDROM drive.

Modern RATs are very simple to use. They come packaged with two files - the server file and the client file. The hacker tricks someone into running the server file, gets his IP address and gets full control over his/her computer. Some Trojans are limited by their functions, but more functions also mean larger server files. Some Trojans are merely meant for the attacker to use them to upload another Trojan to his target's computer and run it; hence they take very little disk space. Hackers also bind Trojans into other programs, which appear to be legitimate e.g. a RAT could be bound with an e-greeting card. Most RATs are used for malicious purposes, such as to irritate, scare people or harm computers, (Forde & Patterson, 2003).

Remote administration Trojans open a port on your computer and bind themselves to it (make the server file listen to incoming connections and data going through these ports). Then, once someone runs his client program and enters the victim's IP address, the Trojan starts receiving commands from the attacker and runs them on the victim's computer. Some Trojans let the hacker change this port into any other port and also put a password so only the person who infects the specific computer will be able to use the Trojan. In some cases, the creator of the Trojan would also put a backdoor within the server file itself so he will be able to access any computer running his Trojan without the need to enter a password (ibid).

Password Trojans search the victim's computer for passwords and then send them to the attacker or the author of the Trojan. Whether it is an Internet password or an email password there is a Trojan for every password. These Trojans usually send the information back to the attacker via Email (Forde & Patterson, 2003).

Privileges-Elevating Trojans are usually used to fool system administrators. They can either be bound into a common system utility or pretend to be something harmless and even quite useful and appealing. Once the administrator runs it, the Trojan will give the attacker more privileges

on the system. These Trojans can also be sent to less-privileged users and give the attacker access to their account, (Forde & Patterson, 2003)

Key loggers are very simple trojans. They log all of the victim's keystrokes on the keyboard (including passwords), and then either save them on a file or email them to the attacker once in a while. Key loggers usually do not take much disk space and can masquerade as important utilities, thus making them very hard to detect.

Joke programs are trojans that are not harmful. They can either pretend to be formatting your hard drive, sending all of your passwords to some hacker, self-destructing your computer, or turning in all information about illegal and pirated software you might have on your computer to the police. In reality, these programs do not do anything.

2.8 EMAIL/INTERNET RELATED CRIMES

2.8.1 Email spoofing

A spoofed email is one that appears to originate from one source but has actually emerged from another source. Email spoofing is usually done by falsifying the name and / or email address of the originator of the email.

2.8.2 Cyber Defamation

This occurs when defamation takes place with the help of computers and / or the Internet. E.g., someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends.

2.8.3 Cyber stalking

The Oxford dictionary defines stalking as "pursuing stealthily". Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat rooms frequented by the victim, constantly bombarding the victim with emails etc.

2.8.4 Threatening emails

Email threats require a criminal to know a victim's email address to send threatening messages either to blackmail him/her or scare the person.

2.8.5 Email bombing

Email bombing refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or servers (in case of a company or an email service provider) crashing.

A criminal achieves this by subscribing the victim's email address to a large number of mailing lists. Mailing lists are special interest groups that share and exchange information on a common topic of interest with one another via email. If a person has been unknowingly subscribed to hundreds of mailing lists, his incoming email traffic will be too large and his service provider will probably delete his account.

2.8.6 Data diddling

This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.

2.8.7 Salami attacks

These attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed. E.g. a bank employee inserts a program, into the bank's servers, that deducts a small amount of money from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizeable amount of money every month.

2.8.8 Denial of Service attacks

Denial-of-service (or DoS) attacks are usually launched to make a particular service unavailable to someone who is authorized to use it. These attacks may be launched using one single computer or many computers across the world. In the latter scenario, the attack is known as a

distributed denial of service attack. Usually these attacks do not necessitate the need to get access into anyone's system (Duke, 1999).

DoS attacking computer can change its source address randomly thereby making it seem as if the attack is originating from many thousands of computers while in reality there may be only a few.

2.8.9 Logic bombs

These are event dependent programs. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs.

2.8.10 Internet time theft

This connotes the usage by an unauthorized person of the Internet hours paid for by another person.

2.8.11 Web jacking

This occurs when someone forcefully takes control of a website (by cracking the password and later changing it). The actual owner of the website does not have any more control over what appears on that website.

2.9 VULNERABILITY TO CYBER CRIMINALS

There are several factors that make users vulnerable to cybercriminals. These factors need to be considered when planning a security protection system. Some of the main ones are listed below.

2.9.1 Physical and virtual security

Any online activity has a physical and a virtual aspect. In the context of crime in cyber space, it is important to consider physical and information technology security together, as it is now impossible to consider one without the other. This remarkable progress has been made by simplifying the user interface, speeding up data transmission and providing greater storage capacity at lower cost. The 'plug and play' cost is low allowing more people to jump onto the

information superhighway. However, some users do not fully evaluate the risks of committing to new technologies. There is a significant gap between the assessment of the value of adopting new technology and the risk involved. The problem is inescapable partly because the criminal uses of new technology are difficult to anticipate and the risks difficult to quantify. Without an appreciation of the likely costs of using new technology or of making technological applications more secure, it is difficult to persuade those who invest in it that there is a downside, (Gold, 1999).

2.9.2 High tech crime

Just as information and communications technologies have provided a platform for social, business and political activity, they also have been readily adopted as a platform for other less pro-social activity. Such technology is a powerful tool for those committing crimes, either by attacking computers or by using them to further other criminal activity. It is often said that there are no new crimes involving computers, rather, new ways of committing old crimes.

Some of the features of high tech crime include: No standard definition of online crimes either nationally or internationally; differences in laws and policing which are exploited to commit crimes; offenders network digitally; many offenders have access to advanced computer skills, some offenders minimise their criminal activity as fantasy; computer crime is a low cost/high volume business which can lead to high levels of damage or profit; criminal activity can be divided into smaller and smaller functional segments that can be grouped and re-grouped at will. Online criminal networks are flatter and less hierarchical than traditional crime groups; the behaviour and tools used by offenders online often have a legitimate use (Grabosky, 1998).

Ordinary users are often unaware of illegal activity affecting them; ordinary users may not know that their identity or computer has been hijacked by an offender. Businesses and householders may be both victims and vectors of high tech crime. The move by criminals to specialize in various aspects of high tech crime is illustrated by the proliferation of malicious software, often developed by sophisticated hackers only to be taken up by less experienced users and launched onto the net infecting vulnerable machines. Trojan Horse software is one

such example as it can be used to compromise machines by taking control of them over the Internet creating a 'bot army' which then can be hired out to spread spam, or commit a denial of service attack on another user, (Denning, 2001).

2.9.3 Hackers

Hackers can steal credit card records or other identifying data, using them directly or selling them to commit identity fraud. Spam or directed attacks can also be used in phishing attacks to obtain access to finances online. The 'mules' or people needed to transfer the money back to the organisers of this sort of criminal activity can also be recruited online and then make their transactions online. All these products and services are now routinely networked among offenders enabling them to commit crimes, (Denning, 2001).

2.9.4 Security threats

A lack of security can lead to criminal attacks on a network including: theft of data; corruption of system integrity; hacking; sabotage; espionage; theft of capacity; and loss or theft of mobile and portable devices. The security threats that affect wireless LANs can be divided into active and passive attacks.

2.9.5 Active attacks

These include: spoofing the authorized access point; denial of service attacks; 'replay attacks' to cause a denial of service, or accelerate data flow to aid in the cracking of WEP encryption; and dictionary attacks to guess the base station SSID (Service Set Identifiers).

2.9.6 Passive attacks

Passive attacks rely on the collection of data in transit without interrupting the communication between authorized devices. A person can launch a man-in-the-middle attack using software that can cause significant disruption and loss. Another example of a passive attack in the wireless environment is the phenomenon of 'war driving'. This is a variation on the older activity of 'war dialling' used to breach telephone systems. A war driver travels around using a

laptop or PDA to locate and possibly exploit connections to wireless networks, (Grabosky, 2000).

2.9.7 Law enforcement challenges

Not all of the costs of high-tech crime control can be met by users, nor can they all be left for law enforcement. From a law enforcement perspective, industry and citizens must work with authorities to keep cyberspace as safe as possible. While methods of policing and immediate priorities have changed over time, the basic ideal of policing is to enforce the rule of law by working cooperatively within, and for, the community. The job of policing can be divided into three areas of prevention detection and investigation, and prosecution. Each of these can be considered in relation to physical and IT security.

2.9.8 Prevention

ICT has been developed without building in from the beginning security mechanisms to protect it from misuse. Consequently, ICT platforms are readily misused and once a criminal application has been developed, it can persist in ways that cannot easily be stopped. As a result, cyber space users are left in a cycle of vulnerability, exploit and patch for each new vulnerability. In the real world, crime-reduction strategies can target the architecture of public places and the ways in which their spaces are patrolled and monitored. In the physical world, it is accepted that police cannot be posted on every street corner. Police have limited influence over the architecture of the wireless environment, (Grabosky, 2000).

Prevention is therefore in the hands of users and the police interest is to ensure that users take into consideration the full impact of their decisions when committing to wireless technology. Most commercial enterprises and government agencies are aware of the need for IT security – the problem for them is deciding what is best, (Report by the Advanced Computing Research Centre (2005a) (2005c).

3.0 RESEARCH METHODOLOGY

3.1 INTRODUCTION

This chapter describes the methodology that will be used as an aid to carrying out the research study. It describes specific strategies that will be used in data collection, analysis in order to answer research questions. It constitutes the blue print of the collection, measurement and analysis of data. It is a plan for selecting the sources and types of information used to answer the research question. It provided answers for such question as; what techniques were used to gather data? What population was studied? What kind of sampling was used? How was data collection and analyzed?

3.2 RESEARCH DESIGN

The research design refers to a strategy to be used by the researcher in collection and analyzing data in order to answer the research questions. This research design will be descriptive research design. Descriptive research includes survey and fact-finding enquiries of different kinds. The major purpose of using descriptive research design in this study is to ensure the description of the state of affairs as it exists at present.

3.3 DESCRIPTION OF POPULATION

The population of the study consists of persons who use the Internet as a tool of communication, business transacting or sources as of information. Another sample of the population includes cyber café owners and persons who hold electronic credit/debit card and use them to transact with these cards.

3.4 THE SAMPLE AND SAMPLING PROCEDURE

The sample is a selection of the population selected for observation analysis. The selected sample represents the target population. The researcher will use random sampling method in selecting the samples of the study.

To determine the sample size from the large target population, the researcher uses accessible population, which in this study refers to computer users and internet/electronic users. The researcher further adopts the approach given by Gay (as cited by Mugenda and Mugenda (1999) who states that for descriptive studies ten percent of the accessible population is enough to give comprehensive study.

The respondents were approached in different ways; information from cyber cafe owners was sourced by approaching cyber cafes within Nairobi. The researcher interviewed the persons responsible for managing the cafe hence they qualified as owners. The electronic card holders' responses will be gathered by approaching shoppers mainly in supermarkets who use credit cards to shop and also approaching persons withdrawing cash from Automated Teller Machines. Lastly, the Internet users were approached in cyber cafes and students who own computers and often use the Internet to access information.

The sample size was calculated in the following manner: -

S/NO	Research sample	Accessed population
1	Cyber cafe' owners	25
2	Electronic card users	60
3	Computer/internet users	100
Total		185

3.5 DESCRIPTION OF DATA COLLECTION TOOLS

The data needed for this study will be both primary and secondary data. Primary data refer to raw data that is being collected for the first time for the purpose of the study. Secondary data refers to data that had previously been collected by other scholars and researchers. The

purpose of collecting this primary data will be to meet the objective of the study. Secondary data will be collected from books, reports on cyber crime and information from the Internet.

Questionnaires are predetermined questions whereby the respondent will be given a chance to fill at their time in response to what they consider necessary or relevant to the questions. In this study the researcher will use the questionnaire method to collect the primary data from the target respondents. A questionnaire designed will contain both open and closed ended semi-structured questions, which will be administered to the target respondents. The main advantage of using this method for collecting primary data is its versatility. It allows collection of large amount of data from the target respondents. It's also fast and saves time. The open-ended question allows the respondent to give in-depth information on the subject of interest.

The questionnaire is structured in a way that, it brings out the various types of cyber crime internet users are faced with, by asking respondents various attacks they have experienced in reference to identified cases of cyber crime. Part A of the questionnaire deals aims to find out if Kenya is a target of cybercrime by determining if respondents have experienced cybercrime. Part B addresses the major types, extent and intensity of cybercrime respondents have experienced including electronic card theft. Part C gives a provision whereby respondents would give opinions on various ways of curbing cyber crime in Kenya.

3.6 DATA ANALYSIS PROCEDURES

All the questionnaires and interviews schedule will be adequately checked for reliability and verification .The researcher will generate information by analyzing data using qualitative and quantitative techniques. This will involve reducing accumulated data to a manageable size by developing summaries, looking for patterns and applying statistical techniques. The data will be analyzed descriptively. This will involve use of pie charts, percentages, graphs and tables among others where applicable. This method will be adapted as it allows the analysis and presentation of large amount of data that will be collected in the field .The researcher will mainly use the computer package excel to analyze the data as stated above and present it in form of pie

charts, graphs, and tables. Documentary sources will be employed whereby the researcher will use previous documents or information to support data received from questionnaires and interviews.

UNIVERSITY OF NAIROBI
EAST AFRICANA COLLECTION

4.0 RESEARCH FINDINGS AND ANALYSIS

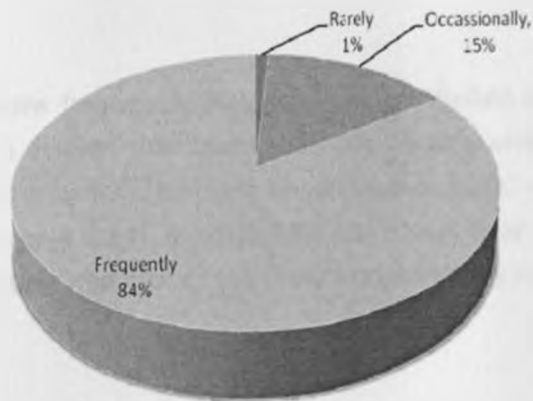
4.1 INTRODUCTION

This chapter gives a detailed analysis of the data collected. It further shows the discussion and results which centre on all the research questions on which data was collected by use of various methods. The questionnaires were distributed so as to attain the target of 25 cyber café owners, 60 card holders and a further 100 internet users. Two procedures were used in data analysis and these were; frequency distribution and percentage distribution. Frequency distribution involves counting the number of the respondents who gave similar response to a given question. Percentage distribution involves conversion of frequency into percentages.

4.2 CYBERCRIME

Respondents were first asked if they had ever experienced any form of cybercrime as an internet user, electronic card holder or cyber café owner/manager. All respondents answered that they had experienced some form of cybercrime. 84% of the respondents had experienced at least one form of cybercrime frequently, 15% experienced in occasionally and 1% experienced it rarely.

Figure 1: Instances of cybercrime

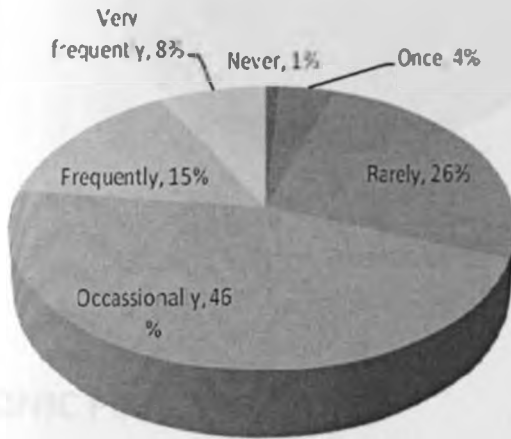


Source: Research Findings

4.3 BLACKMAIL EMAILS

The respondents were asked whether they had received any form of blackmail emails. The response was as follows. From Figure 2, at least 69% of respondents reported to having received blackmail e-mails from various sources.

Figure 2: Blackmail E-mail received

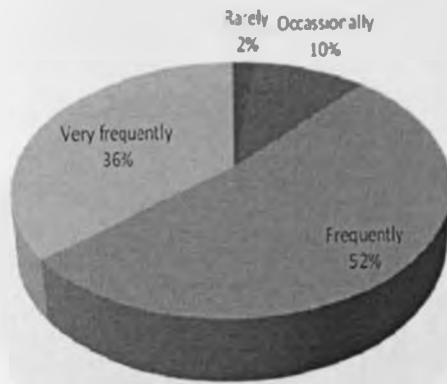


Source: Research Findings

4.4 SPAM

Internet users were asked how frequently they received unsolicited e-mails and the responses are captured in table 3. It is evident that spam is a considerable problem of cyber crime with 88% of those interviewed frequently receiving unsolicited e-mails. An additional 10% of the respondents occasionally receive spam. In total, 98% claim that they have received some form of spam, thus making it a strong indicator of the cyber crime activity in Kenya.

Figure 3: Unsolicited e-mails

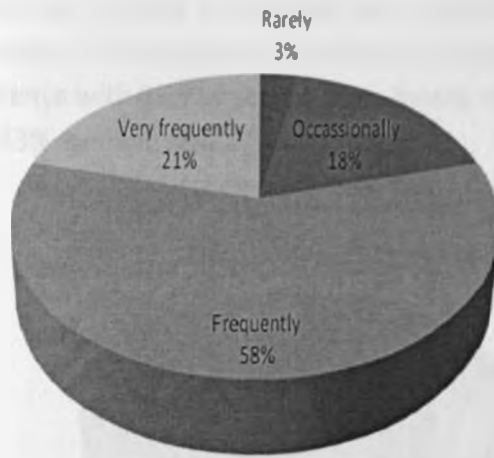


Source: Research Findings

4.5 ELECTRONIC PIRACY

In a bid to determine the extent of electronic piracy, respondents were asked if they had ever used pirated electronic material such as software. As depicted in Figure 4 below, electronic piracy in the country is rampant as a form of cybercrime with all respondents having used pirated material, 79% of who have used the material frequently and very frequently. Only 3% said that they used it rarely.

Figure 4: Usage of Pirated Material

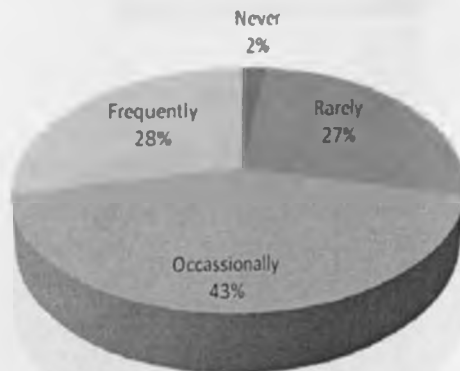


Source: Research Findings

4.6 DENIAL OF SERVICE

To find out the extent of denial of service, internet users were asked how frequently they experienced a defaced website or an inaccessible website. From Figure 5 below, only 2% of the respondents have never experienced denial of service as a form of cybercrime. Of the 98% who experienced denial of service, 28% of them experienced it frequently.

Figure 5: Denial of Service

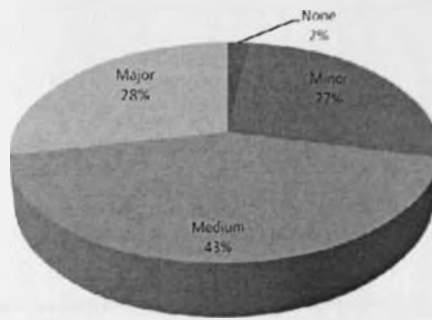


Source: Research Findings

4.7 SALES AND INVESTMENT FRAUD

Respondents were asked up to what levels they had received bogus sales and investment information over the internet. The responses as depicted in Figure 6 below shows that this form of fraud is prevalent in Kenya with 98% of respondents having received fraudulent information, 28% being major fraud, 43% medium and 27% minor.

Figure 6: Sales and Investment Fraud

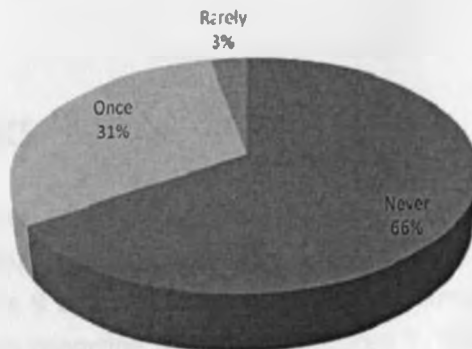


Source: Research Findings

4.8 TELEPHONE SERVICE THEFT

The research investigated instances of telephone service theft and the responses as seen in Figure 7 reflected that this is not a major form of cybercrime in Kenya. 66% of the respondents have never experienced this form of theft. Of the 34%, only 3% have experienced it rarely and 33% only once.

Figure 7: Telephone service theft

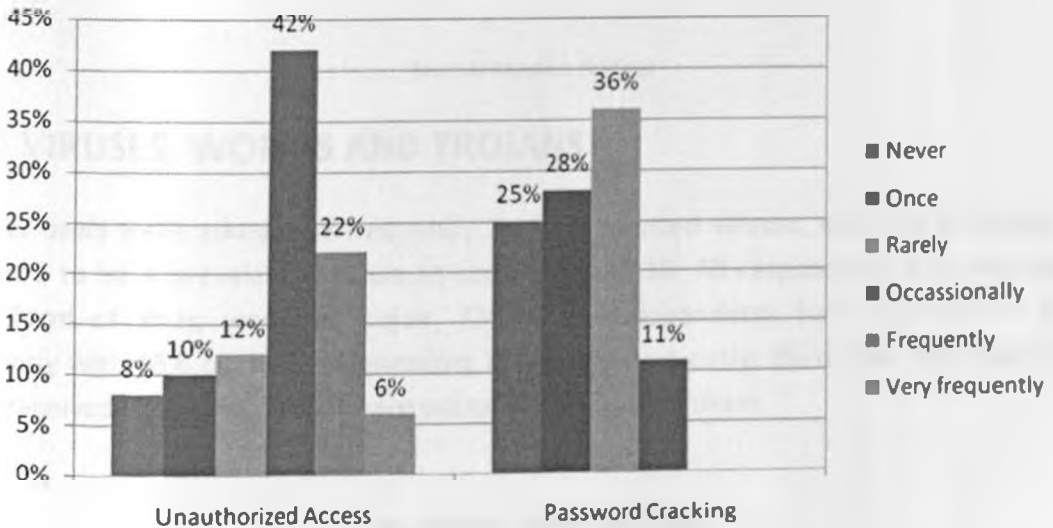


Source: Research Findings

4.9 HACKING

In a bid to find out the extent of intrusion of privacy, respondents were asked how frequently they experienced two forms of hacking, unauthorized access and password cracking. According to Figure 8 below 70% of the respondents experienced unauthorized access occasionally. 8% of the respondents have never experienced it while 22% experienced it once or rarely. Password cracking was only experienced occasionally by 11% of the respondents, rarely or once by 53% and never by 25%. This shows that unauthorized access is majorly experienced in hacking as compared password cracking.

Figure 8: Instances of hacking



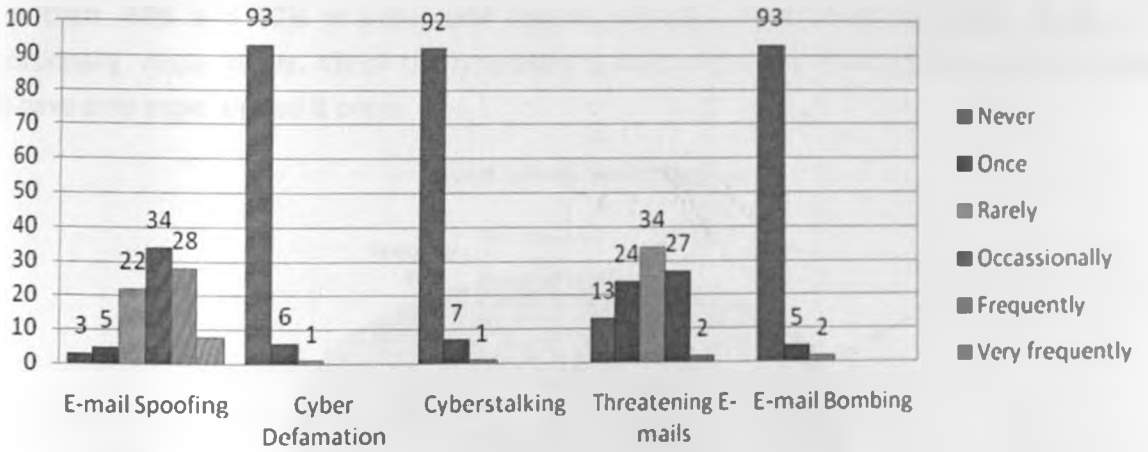
Source: Research Findings

4.10 EMAIL ATTACKS

To determine the instances of e-mail attacks respondents were asked how frequently they experienced e-mail spoofing, cyber defamation, cyber stalking, threatening e-mails and e-mail bombing. As seen in Figure 9 below, E-mail spoofing was the most prevalent of email attacks with 97% of all respondents reporting having experienced it, followed by threatening mails with 87% of respondents having received such e-mails. Cyber defamation and e-mail bombing were

the least experienced attacks with only 7% of all respondents having experienced them, albeit rarely. Cyber stalking is also rare, with only 8% of all respondents experiencing it.

Figure 9: E-mail attacks

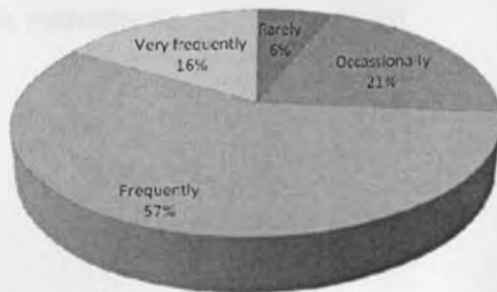


Source: Research Findings

4.11 VIRUSES, WORMS AND TROJANS

Internet users were asked how frequently they experienced viruses, worms and Trojans. This appeared to be a prevalent problem as seen in Figure 10. All respondents have experienced some form of virus, worm or trojan. 73% of the respondents have experienced viruses frequently with 16% of them experiencing them very frequently. 6% of the respondents have rarely received viruses while 21% have occasionally received them.

Figure 10: Viruses, Worms and Trojans

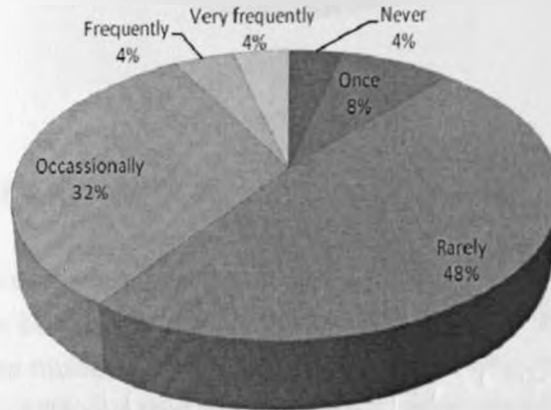


Source: Research Findings

4.12 INTERNET TIME THEFT

25 Cyber café owners were asked how frequently they experienced internet time theft. They rarely had this problem with only 8% of the total respondents frequently experiencing internet time theft. 48% and 32% of cyber café owners experienced internet time theft, rarely and occasionally, respectively. 4% of the respondents have never experienced this problem while 8% have only experienced it once.

Figure 11: Internet time theft

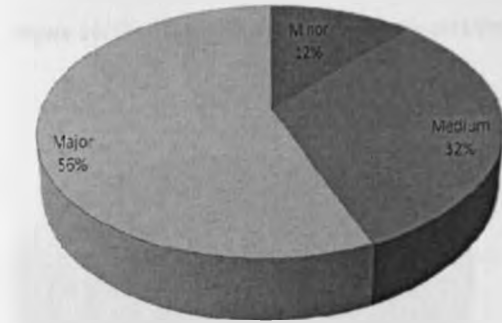


Source: Research Findings

4.13 LEVEL OF RISK OF CYBERCRIME

Cyber café owners and internet users were asked what level of risk they would rate cybercrime as having over their cafe or computer. The responses lead to the conclusion that the respondents consider cybercrime to be a serious problem, with 56% of all of them saying the level of risk of cybercrime is major. 32% and 12% of respondents only consider cybercrime as a medium and minor problem, respectively.

Figure 12: Risk of cybercrime

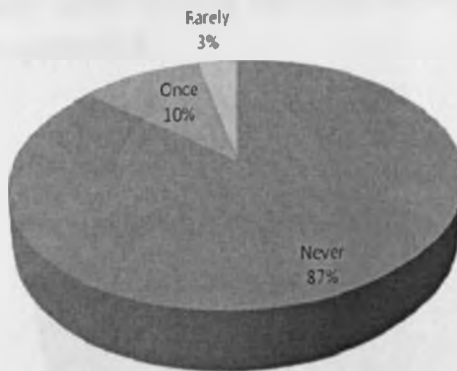


Source: Research Findings

4.14 ELECTRONIC CARD THEFT

The researcher investigated how many card holders, cards being credit, debit, ATM or reward cards, had been attacked by cyber criminals through use of personal information found in the cards, to purchase or use money without permission. According to Figure 13 below 60 card holders responded where 87% said that they had never experienced electronic card theft, 10% have experienced theft while 3% said that they experienced it rarely.

Figure 13: Electronic card theft

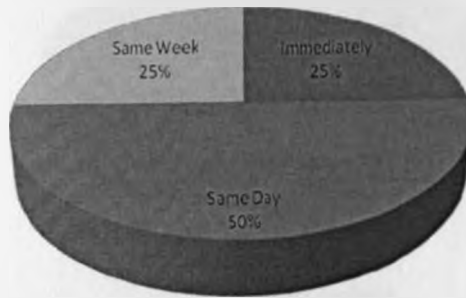


Source: Research Findings

Respondents were also asked how long it took them to discover that they had been victims of electronic card theft. A relatively high level of alertness was reported, with 25% of them

discovering immediately, 50% on the same day and the other 25% discovering the theft during the same week of the theft.

Figure 14: Time taken to discover electronic card theft



Source: Research Findings

4.15 GOVERNMENT ACTION

In order to find out opinion on the role the Government is playing in the fight against cybercrime, internet users, cyber café owners and electronic card holders were asked if they thought the Government is doing enough to curb cybercrime. Most of the respondents, 78%, do not believe that the Government is doing enough to curb cybercrime. 10% think the Government is doing enough while 12% do not know whether or not the Government is involved in the fight against cybercrime.

Figure 15: Government action



Source: Research Findings

They were also asked if they would report cases of cybercrime to the authorities. According to Figure 16 below, 68% said they would not bother reporting while 32% said they would. This

shows that they do not believe that the authorities have the necessary mechanisms to fight cybercrime.

Figure 16: Reporting cases of cybercrime



Source: Research Findings

5.0 RECOMMENDATIONS AND CONCLUSIONS

5.1 INTRODUCTION

The overall aim of the project was to find out if cybercrime has infiltrated developing countries with Kenya being the case study. Despite the difficulty in quantifying this cybercrime, it is obvious from the results of the research that it is becoming a major problem in Kenya.

In the Kenyan context, perhaps the most evident variance between the law and Internet use centres on publication and consumption of prohibited material. Of even greater concern is the use of the Internet as a channel for illegal exploitation of intellectual property. A cursory study of any public cyber facility in Nairobi will reveal widespread popularity of what are commonly known as peer-to-peer networks - internet sites via which vast communities of net users freely swap pirated data, software, music and audio-visual material.

Though Cybercrime in Kenya is yet to manifest itself in the proportions as observed in the western world, it is worth noting that incidence of these is likely to go unreported due to lack of confidence in the law enforcers as shown by the research. There is also the tendency of corporate victims to cast a shroud of secrecy over attacks against them to avoid perceptions of ineptitude and diminished credibility.

There are various contributing factors. They include prevalence of opportunities, weak guardianship, ineffective legislation and extra-territorial issues. Kenyans, who are regularly online, would be well advised to take note of these factors.

The perverts are now capitalising on the gullibility of children, who are increasingly using the Internet as a way of exploring the world with the help of technology. They are also without regard and can easily reveal their personal details, including age, to strangers on the Internet. Whenever these children stumble upon a pornography site, this usually unlocks an avalanche of new pornography windows, making it an addictive vicious circle.

As battle on pornography rages, the immoral material is readily available, with some cartels specialising on perverting young minds. Some cyber cafe operators and parents are now blocking some of the notorious pornography sites to protect children. Whenever one attempts to access these sites, a message appears on the screen warning that access cannot be allowed, (The Standard, May 19, 2005).

Unlike Kenya, Indian policemen are allowed to search cyber cafes and Internet users' homes without warrants at any time, as part of their criminal investigations. This is backed by Parliament's approval of the Information Technology Law in May 2000 to crackdown Cybercrime in the country. The House also allowed the authorities to block access to sites considered pornographic or that which "endanger public order, the integrity and security of the nation and relations with other countries". Those setting up "anti-Indian" websites can be jailed for up to five years.

In China, the government has ordered a crackdown on electronic pornography starting October 1. Police have closed about 700 websites and arrested 329 suspects since the operation started in July.

5.2 THE CURRENT LEGAL SITUATION

There is no law in Kenya governing digital signatures and electronic contracts. Encryption technology can be imported into the country, there is no government requirement for the keys to be stored by a government agency and there is no restriction on the encryption key size. Kenya is not a signatory to any agreements on encryption technologies and there is no clear government policy on the use of encryption technology.

Legislation must be introduced that provides for unauthorized access to a computer or computer system, destruction or alteration of data within a computer system, interference with lawful use of a computer or a computer system and theft of intangible property. Kenya needs to develop its legislation so as to effectively protect electronic commerce. The judiciary should also permit the admissibility of electronic evidence in judicial proceedings.

5.3 THE EVIDENCE ACT

The current state of our legislation is dismally wanting as far as the protection of our collective and individual interests relating to the electronic domain are concerned. Save for section 2 of the Evidence Act (after amendment 69 of 2000), which makes a comprehensive definition of the word 'computer' for purposes of the act, our entire body of statute law remains entirely oblivious of the pervasive changes and developments wrought by the digital era.

However, some electronic crimes inherently feature a non-electronic element that, by extension or analogy, places them within the ambits of existing legislation. For instance, the most of common Internet frauds fall under section 313 of the Penal Code, which sanctions obtaining by false pretences. The same applies to the various forms of fraud, extortion and theft commonly perpetrated by electronic means. Similarly, There is also no doubt concerning the proscriptive adequacy of existing laws on illegal distribution of copyrighted material, and publishing of libellous, seditious or obscene material.

UNIVERSITY OF NAIROBI
EAST AFRICANA COLLECTION

The problem, however, is not one of prohibition, but of enforcement. The nature of the World Wide Web and the ever-compounding complexity of electronic systems make the virtual arena difficult to administer accordingly complicating the investigation and prosecution of Cybercrimes, a situation aggravated by the lack of a statutory structure to address these intricacies.

To reconsider the prohibitive aspect of our laws, the inadequacy of our legislation turns out to be even more serious when we consider the lack of analogy between most Cybercrimes and their conventional counterparts. For instance, the penal sanction against trespass or breaking and entry cannot hold against an act of hacking into a computer network and unlawfully acquiring proprietary data. Similarly, the act of perpetrating a DoS attack or distributing a destructive virus lacks crucial elements of malicious damage to property and cannot be prosecuted.

This situation discloses the need for a comprehensive framework of legislation addressing specific threats to electronic activity and infrastructure. This is important for two reasons, the first being to pre-empt the rise of Cybercrime in its most nascent stages.

5.4 REGIONAL AND GLOBAL INVOLVEMENT

There is the need to act in concert with the global community in combating Cybercrime. Presently, if a fugitive international cyber criminal were to operate from or flee into Kenya, our legislative vacuum would effectively provide such wrongdoer with safe haven. This is an implication of the principle of dual criminality, under which international law requires that whenever one state requests another for the extradition of a criminal in the latter's territory, the act in question must be criminal in both the requesting and the requested state.

A comprehensive framework of anti Cybercrime legislation is needed to safeguard moral standards, proprietary interests, privacy and the integrity of national security and healthy foreign relations, which are increasingly at stake as digital technology continually extends its influence over our day to day activities.

Apart from criminalising certain acts, such a system would further bolster related spheres of legislation to make them relevant to the intricacies and challenges posed by electronic age law and order. For instance, provisions of the Criminal Procedure Code on preventive action by the police including search and entry need to be updated to accommodate the minutiae of investigating electronic crime.

Further, statutes must address certain acts that, though not criminal of themselves, involve deliberate or negligent facility to the perpetration of Cybercrimes; distribution of software used for illegal purposes, hosting of websites that provide resources for cyber criminals and dissemination of information that encourages or informs the commission of Cybercrime.

Only such a legislative structure, one that adequately captures emerging ethical notions that delineate minimum rights and liabilities of Internet users, can properly lay the juridical foundation for a predisposition to IT-driven national development.

SPAM is widely acknowledged as one of the biggest problems facing the World Wide Web (and its potential for socio-economic development). One of the problems in controlling spam is that there is no internationally accepted policy and legal framework for dealing with spam. Attempts by countries in Europe and the USA to deal with spam have made developing countries targets for spammers. Many of these now operate out of these countries to avoid prosecution.

Much work has been done on SPAM especially in the advanced economies, and different countries including the UK and the USA have congressional acts and parliamentary directives specifically devoted to combating SPAM. In the USA, the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act) came into effect on January 1, 2004. The European parliament on 20 May 1997 issued Directive 97/7/EC that deals primarily with issues of unauthorized mails between its member countries and several EU countries have adopted a version of this directive.

In developing countries, especially in Africa, such laws, which arise because of a prior investigation of the nature of the problem of SPAM and its implications for e-commerce, are not present. To counter this, Kenya needs to borrow a leaf from countries that have made the laws on the SPAM issue to contain it.

It is worth noting that Kenya is in advanced stages to assemble a cyber-crime laboratory for police in Eastern Africa States to arrest Internet crime.

5.5 THE CHALLENGE

The scope of international cooperation is currently limited by international agreements and by the national law of the States. There are also differing priorities between developed and developing countries. These differences complicate international cooperation and expand the gap between the two groups on a united fight against Cybercrime.

Another area where problems present themselves is in criminal investigations. Such problems include limited availability of specialized computer crime units; possible lack of powers to investigate the content of a computer system against the will of a right holder; encryption

policies; and verification of authenticity of evidence. Only a universal agreement would enhance the prospects of establishing an international legal instrument in the field in the end.

There is no authoritative, comprehensive elaboration of the principle of universal jurisdiction concerning cyber-crime. There are different views concerning the offences that constitute crimes under international law that are subject to universal jurisdiction.

There are also different opinions with respect to the significance of the obligation to prosecute or extradite, as contained in various treaties, as evidence of universal jurisdiction.

5.6 THE FUTURE OF CYBERCRIME

Preventive measures should focus on the following key trends:

The rapid evolution of Cybercrime will continue. Driven by technology and the creativity of offenders, new schemes will spread rapidly over the Internet. This will pose challenges for domestic and international law enforcement bodies and for the development of international legal standards.

Traditional crime patterns will change. Some crimes, such as fraud and child pornography that are currently limited by language barriers, will expand in scope as language translation software becomes available. As the use of networks gradually shifts from purely informational to electronic commercial activities, crime patterns will follow suit. New opportunities for fraud and money-laundering offences will be created.

Transnational crime will increase. Networks make cross-border crimes easier to commit and bring them within reach of individual offenders. There will be an increase in minor transnational offences committed by unsophisticated offenders. This will put a serious strain on traditional frameworks for extradition and mutual legal assistance, which are not equipped to handle the caseloads.

Organized crime will take advantage of the changes. Transnational organized crime uses networks since they provide relatively secure media for communication, the concealment of

evidence and the electronic movement of money of illegal origin. Data can be encrypted and used to thwart law enforcement.

Not all-transnational computer crime will be "organized crime". Computer networks open opportunities that allow individual offenders to commit sophisticated crimes that were once associated with organized crime. Networks may also support entirely new forms of criminal organisations that do not fit within existing legal definitions or approaches. One implication of this is that, while the *U.N. Convention against Transnational Organized Crime* will be a valuable precedent in some areas, a global instrument on cybercrime will have to break new ground in others. It will have to deal effectively with individual criminals and not just organized criminal groups.

5.7 CHALLENGES FACING THE INTERNATIONAL COMMUNITY AND THE PRIVATE SECTOR

Addressing these problems require a concerted effort from national governments and the international community as a whole. The need for universality and for a forum in which all countries can participate in drawing up policies, legal reforms and technical solutions suggests that the United Nations will be called upon to play an important role.

Aggressive strategies are needed to protect the technology itself from such things as "hacking," invasions of privacy and the propagation of harmful programs such as computer viruses. New methods of creating, transmitting and storing information also raise issues. Copying of data has led to pressures to prosecute copyright infringement. The lack of control has exacerbated the transmission of "offensive content" such as hate propaganda or content considered blasphemous, subversive, pornographic, or as inciting or assisting in the committing of crimes. Religious and cultural differences will also play a role in developing international policies against crime.

A strategy for combating computer crime will have to incorporate investigative powers that could be used to obtain evidence from anywhere on a computer network -- regardless of

national jurisdiction -- more quickly than offenders can either move or erase evidence. At the same time, there should be national and international requirements for the protection of privacy, freedom of expression and other basic human rights. This will be particularly difficult because at present the most effective human rights protections in criminal cases are codified in national laws and constitutions and enforced by national courts ill-equipped to deal with transnational cases.

Most security and crime control measures on the Internet consist today of technical standards set by the industry itself, irrespective of political pressures or basic human rights protections. The private sector also tends to generate effective crime controls where they are needed for commercial reasons, but not where the controls would interfere with easy customer access or would increase operating costs. There is a risk that developing countries may be excluded by the industry itself because they are not able to effectively control domestic computer crime or because they cannot meet technical security requirements for communications or electronic commerce.

Perhaps the greatest challenge to developing an effective global strategy will be to train skilled investigators and prosecutors and keep them up to date on the latest technological and criminal developments. This effort strains even wealthy and technically-advanced countries, and expertise will be needed to avoid legal loopholes that electronic offenders can exploit. In the ultimate analysis, our goal should be to ensure that everyone can participate in the electronic community without the fear of being victimized.

5.8 LIMITATIONS OF THE STUDY

The limitations of the study can be summarised as follows:

5.8.1 Responses

Not all of the potential respondents who were approached were willing to answer the questions.

5.8.2 Technical Jargon

Some of the terms used in the questionnaire were not self explanatory and the researcher had to explain to some of the respondents what they meant. Such terms include telephone service theft, Email spoofing, Cyber Defamation, Cyber stalking, and Email bombing.

5.8.3 Sectoral Limitations

The generalisation of the study required collecting data mainly from users. Since other players in the industry such as web developers, system administrators and network engineers were not included in the research then the study may not be considered to be wholly representative of the Kenyan situation.

5.9 RECOMMENDATION FOR FURTHER RESEARCH

Cybercrime is a wide area that affects several sectors of the economy. The research base should therefore be widened to cover other players in the sector other than users.

During the course of the research, it was discovered that there were numerous forms and ways of cybercrime such as identity theft through phishing and pharming, which could not be adequately covered.

Despite the limitations, Kenya is slowly accepting the prevalence of cybercrime and steps are being taken to curb it. This work therefore sets up future contributions that will enable ICT Policy makers, institutions and users protect themselves from cybercrime.

BIBLIOGRAPHY

- British Broadcasting Corporation (BBC). (2007). *Hackers Target TK Maxx Customers* retrieved on July 10, 2008 from <http://news.bbc.co.uk/2/hi/business/6508983.stm>.
- Coastweek. (2007). *Break-in at Pastoral Centre Offices* retrieved on July 17, 2007 from <http://www.coastweek.com/3018-16.htm>
- Creed, A. (1999). Indonesian Govt Suspected In Irish ISP Hack, *Newsbytes* February 21, 1999 Retrieved July 8, 2007 from <http://www.ccurrents.com/newstoday/99/02/21/news8.html>
- Denning, D. E., & Baugh, W. (1997). *Encryption and Evolving Technologies: Tools of Organized Crime and Terrorism*, Working Group on Organized Crime, National Strategy Information Center Washington.
- Gold, S. (1999). BT Starts Switchboard Anti-Hacking Investigation. *Newsbytes* Jan 11 retrieved on August 12, 2008 from <http://www.infowar.com>.
- Grabosky, P. N., & Smith, R. (1998). *Crime In The Digital Age: Controlling Telecommunication And Cyberspace Illegalities*, Transaction Publishers. New Brunswick.
- Grant, A., David, F., & Grabosky, P. (1997). *Transnational Organized Crime*. Vol. 3, No. 4, Frank Cass & Co. London.
- Grant, A., David, F. & Grabosky, P (1997). *Child Pornography in the Digital Age*. *Transnational Organized Crime*, vol. 3, no.4 pp 171 - 188. Frank Cass & Co., London.
- Hundley, R. and Anderson, R. (1995). *Emerging Challenge: Security and Safety in Cyberspace*. *IEEE Technology and Society Magazine*, 14,4: 19-28.
- Kumar, A. (2002). *Cybercrime - Crime Without Punishment*. Retrieved from Inomy site: <http://www.inomy.com>
- Mathew, N. (2005). Law On Cybercrime Overdue. *Legalweek*. Computer Crime Research Centre retrieved on July 9, 2008 from <http://www.crime-research.org/news/22.02.2005/982/>.
- Meyer, M., Underwood, A. (1994). Crimes of the Net, *Newsweek*, November 15 1994 pg 68-69

- Muniata, P. (2004). Visa Says Credit Card 'Not Widespread'. *The East African* May 10, 2004
retrieved on August 8, 2007 from
<http://www.nationaudio.com/News/EastAfrican/current/Business/Business1005200434.html>
- Newman, K. (1998). Phone Call Scams Skim off Millions. *New Zealand Herald* August 8, 1998
Retrieved on July 9 2008 from <http://www.infowar.com>
- Price Water House Coopers (2002). An Economic Crime Survey In Zambia, Tanzania And Kenya,
Fraud and Corporate Crime retrieved on July 10, 2007 from
<http://www.aic.gov.au/stats/crime/fraud/africa.html>
- Rathmell, A. (1999). Cyber-terrorism: The Shape of Future Conflict? *Journal of Financial Crime*
Vol. 6, Issue. 3, retrieved on July 10, 2007 from
<http://www.emeraldinsight.com/10.1108/eb025897>
- Schieck, M. (1995). Combating Fraud in Cable and Telecommunications, *IIC Communications*
Topics No. 13. London: International Institute of Communications.
- Tendler, S. and Nuttall, N. (1996). Hackers Leave Red-Faced Yard with \$1.29m Bill, *The Australian*, 6 August: 37.

APPENDICES

APPENDIX A: INTRODUCTORY STATEMENT

I am a student of the University of Nairobi undertaking a course on Strategic and Security Studies and I would like to ask you some questions regarding to Cybercrime. Please be assured that this discussion is strictly confidential, the information gathered will never be linked back to you and you may choose to stop the interview at any time. Whatever information you provide will be used purposely for coursework evaluations and will be seen only by staff and lecturers of University Of Nairobi.

Participation in this survey is voluntary and you can choose not to answer any individual question or all of the questions. However, I hope that you will participate in this survey since your views are important.

You are free to ask any questions before you answer the subsequent questionnaire.

Chebiegon Kangogo

APPENDIX B: QUESTIONNAIRE

Code.....

Name (*optional*).....

Date.....

Physical Address.....

Section A

1. Tick the category which defines your role/ position,

- | | |
|---------------------------|-----|
| Internet user | [] |
| Electronic card holder | [] |
| Cyber cafe owner/ manager | [] |

UNIVERSITY OF NAIROBI
EAST AFRICANA COLLECTION

2. Have you ever experienced any form of cyber crime?

Yes []

No []

3. How could you rate the frequency of cyber crime attacks you have experienced?

Rarely []

Occasionally []

Frequently []

Section B

I.

1. To what extent does conspiracy or black mail emails get into your email box?

Never []

Once []

Rarely []

Occasionally []

Frequently []

Very frequently []

2. How often do you receive offensive materials in your inbox which you didn't solicit for?

Never []

Once []

Rarely []

Occasionally []

Frequently []

Very frequently []

3. How often have you used pirated electronic material such as software programs and music?

Never []

Once []

Rarely []

Occasionally []

Frequently []

Very frequently []

4. To what extent have you experienced a defaced website or inaccessible website?

Never []

Rarely []

Occasionally []

Frequently []

5. To what level have you received bogus Sales and Investment Fraud through cyberspace?

None []

Minor []

Medium []

Major []

6. How often do you experience telephone service theft?

Never []

Once []

Rarely []

Occasionally []

Frequently []

Very frequently []

7. Among the listed modes of cybercrime by criminals, which one have you experienced and to what level? (Grading them on a scale of 1-6, 1-Never 2-Once, 3-Rarely, 4-Occasionally 5-Frequently & 6- Very Frequently)

Unauthorized Access _____

Password cracking _____

8. As an internet user, how often have you experienced the following email attacks and to what level? (Grading them on a scale of 1-6, 1-Never 2-Once, 3-Rarely, 4-Occasionally 5-Frequently & 6- Very Frequently)

Email spoofing _____

Cyber Defamation _____

Cyber stalking _____

Threatening emails _____

Email bombing _____

9. To extent have you experienced viruses, worms and Trojans as an internet user?

Never []

Once []

Rarely []

Occasionally []

Frequently []

Very frequently []

10. As a cyber cafe manager have you experienced Internet time theft, if yes, how often?

Never []

Once []

Rarely []

Occasionally []

Frequently []

Very frequently []

11. What level of risk would you rate cybercrime as having over your cafe or computer?

Minor []

Medium []

Major []

12. What security measures have you taken to prevent and eliminate cybercrime attacks?

II.

1. To what extent have you experienced electronic card theft?

Never []

Once []

Rarely []

Occasionally []

Frequently []

Very frequently []

2. How long did it take to realise you have been a victim of electronic card theft?

Immediately []

Same day []

After a week []

Long over-due []

3. Do you think you area an easy target for electronic card theft? Why?

4. What measures have you taken to protect yourself from electronic card theft?

Section C

1. Do you think the government has done enough to curb cybercrime?

Yes. []

No. []

Don't Know []

2. Have you ever or would ever report any Cybercrime cases to the authority?

Yes. []

No. []

3. Do you have any suggestion regarding what one should do to protect him/her from cybercrime?
