

93625

HV
6773
1059
2013

**BUSINESS REACTIONS TO CYBER SECURITY THREATS IN THE KENYA
BUSINESS ENVIRONMENT**

By

CELESTINE MOIGE ONWONG'A

**A Research Thesis Submitted in Partial Fulfilment of the Requirements for the
Degree of Master of Commerce at Strathmore University**

**School of Management and Commerce
Strathmore University,
Nairobi Kenya**

April, 2013

This thesis is available for Library use on the understanding that it is copyright material and that no quotation from the thesis may be published without proper acknowledgement.

Declaration and Approval

I declare that this work has not been previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made in the thesis itself.

Signed CM Date 24/03/2013

Celestine Moige Onwong'a

Approval

This thesis was reviewed and approved by the following:

Dr Vincent Omwenga

Senior Lecturer, Faculty of Information Technology

Strathmore University

Mr. David Wangombe

Dean School of Management and Commerce

Strathmore University

Professor Ruth Kiraka

Dean School of Graduate Studies

Abstract

The global wave of information and communication technologies (ICT) has brought enterprises not only enormous benefits, but also linked information threats. This thesis discusses the reactions of businesses to these cyber security threats in the Kenya business environment. More specifically it examines the characteristics of cyber security threats, the awareness levels of the Kenya business community to these threats, the manifestation of cyber security threats and the overall business reactions to the threats. The empirical study was conducted in businesses across 12 different sectors within Nairobi County between November 2012 and January 2013. It targeted IT specialists and internal auditors from each of the sampled businesses totaling 83 respondents. The research adopted a descriptive and correlational design. Data obtained was analyzed using descriptive statistics. The analytical results revealed that business reactions are pegged on the realization of the internet as a “double-edged sword”, which provided many opportunities for individuals, organizations and governments to develop but with it brought endless opportunities for cyber criminals to exploit. The research argues that cyber threats, with their unique characteristics, present new challenges to law enforcement, organizations and society as a whole. The study also finds that firms have reacted to this ‘new’ risk by putting in place various cyber security measures e.g. having in place policies and guidelines, installing various technological tools like anti-viruses with an aim to deter, prevent and detect cyber security threats. More is yet to be done by the various stakeholders in Kenya so as to secure the cyber environment. This study recommends an extension of the study to small and medium-sized organizations as it would enhance the generalizability of the findings. Different parts of the country could also be considered for future research for comparability purposes.

Definition of key terms

Cyber security threat- refers to a potential violation of security where computers or networks act as the tools, target or place of criminal activity (ITU, 2012).

Business reaction- refers to the business' use of countermeasures as the response to cyber criminals' stimulus (Stalings, 2006).

Table of Contents

Declaration and Approval.....	iii
Abstract.....	iv
Definition of key terms	v
Table of Contents.....	vi
List of Tables	xii
List of Figures	xiii
List of Abbreviations	xiv
Acknowledgement.....	xvi
Dedication	xvii
CHAPTER ONE.....	1
INTRODUCTION	1
1.1 Background	1
1.1.1 Brief History of Cyber Security Threats and Cyber Security	2
1.1.2 Business in a Cyber Environment in Kenya	4
1.1.3 Various aspects on cyber security	5
1.1.4 Cyber security in Kenya	8
1.2 Theories in cyber security	12
1.3 Statement of the problem	13
1.4 Research objectives	14

1.5 Research questions	14
1.6 Significance of the study.....	15
1.7 Justification for the study	16
1.8 Scope of the study.....	16
CHAPTER TWO.....	17
LITERATURE REVIEW	17
2.1 Introduction.....	17
2.2: Factors influencing Organization's cyber security practice.....	17
2.2.1 Costs versus benefits	17
2.2.2 Organization's Dependence on IT.....	19
2.2.3 Nature of sector.....	20
2.2.4 Diverse User Needs	21
2.2.5 Size of the Business	21
2.2.6 Vulnerability of Specific Business Sectors	22
2.2.7 Existence of Legislations.....	22
2.2.8 Financial Position.....	23
2.2.9 Knowledge.....	23
2.3 Characteristics of cyber security threats.....	23
2.3.1 Borderless.....	23
2.3.2 Unobserved Ethical Boundaries	24

2.3.3 Difficulty in Establishing Person Responsible	24
2.3.4 Difficulty in prosecuting offenders	24
2.3.5 Threats have a Multiplier Effect	25
2.3.6 Low Cost.....	25
2.3.7 Few Reported Cases.....	25
2.3.8 Anonymity	26
2.4 Manifestation of Cyber Security Threats.....	26
2.4.1 Types of Cyber Security Attackers:	26
2.4.2 Cyber Security Threats.....	28
2.5 Effects of Cyber Security Threats	34
2.5.1 Direct Effects.....	34
2.5.2 Indirect Effects.....	35
2.6 Businesses Reactions to Cyber Security	36
2.6.1 Cyber-crime Combating Approaches	36
2.7 Research Conceptual Framework	43
CHAPTER THREE.....	45
RESEARCH METHODOLOGY.....	45
3.1 Introduction.....	45
3.2 Research Design	45
3.3 Population and Sampling.....	46

3.4 Data collection	47
3.5 Data Analysis and Presentation	47
3.6: Reliability, Validity and Objectivity of the Research	48
3.7 Ethical Issues	49
CHAPTER FOUR	51
RESEARCH FINDINGS	51
4.1: Introduction	51
4.2 General Information	52
4.2.1 Job Description of the Respondents	52
4.2.2 Duration of Service to an Organization	53
4.2.3 Primary Function of the Organization.....	54
4.3 Analysis of Cyber Security Threats' Characteristics.....	54
4.3.1: Characteristics of Cyber Security Threats	55
4.3.2 Rapid spread of Cyber Security threats.....	56
4.4 Awareness of Cyber Security Threats	57
4.4.1 Awareness	57
4.4.2 IS Security Plan	58
4.4.3 Budget Allocation.....	58
4.4.4 Rating an organization's implementation of cyber-space security	60
4.4.5 Cyber Space Security Strategies.....	61

4.4.6 Cyber Security Strategies in Line with Environmental Requirements	62
4.4.7 Cyber Security Strategies in Line with CCK Requirements.....	63
4.4.8: The Cyber Security Primary Function	64
4.4.9: Composition of Information Security Team.....	65
4.5: Manifestation of Cyber Security Threats in a Business Environment.....	67
4.5.1: Manifestation of Cyber Security Threats	67
4.5.2: Effects of Manifested Cyber Security Threats	72
4.6: Business Reactions to Cyber Security Threats	74
4.6.1: Technical approaches	74
4.6.2: Non-technical Measures	75
4.7: Correlation findings.....	77
CHAPTER FIVE.....	80
DISCUSSION, CONCLUSION AND RECOMMENDATIONS.....	80
5.1 Introduction.....	80
5.2: Summary of Findings.....	80
5.3: Conclusion	82
5.4: Research implications	85
5.5: Limitations of the Study	88
5.6: Recommendations for Further Research	88
REFERENCES	89

APPENDIX 1: Introduction Letter.....	97
APPENDIX 2: Respondents' Sector Distribution	98
APPENDIX 3: Frequency of Occurrence of Cyber Security Threats	99
APPENDIX 4: Business Reactions as Relates to Different Sectors	100
APPENDIX 5: Questionnaire.....	101

List of Tables

Table 1.1: History of cyber crime	2
Table 2.1: Cost versus benefit	18
Table 2.2: McFarlan's Grid	20
Table 2.3: Direct effects of cyber security threats	35
Table 2.4: Organizational Measures	43
Table 4.1: Characteristics of Cyber Security Threats.....	55
Table 4.2: Table of Spread of Cyber Security Threats	56
Table 4.3: Cyber security primary function	64
Table 4.4: Manifestation of malware	68
Table 4.5: Manifestation of cyber laundering	68
Table 4.6: Manifestation of Denial of service	69
Table 4.7: Manifestation of phishing	70
Table 4.8: Manifestation of identity theft	71
Table 4.9: Manifestation of System interference.....	71
Table 4.1.0: Effects of manifested threats.....	73
Table 4.1.1: Technical approaches.....	74
Table 4.1.2: Non-technical Measures	76
Table 4.1.3: Cyber security threats versus industry affiliation.....	77
Table 4.1.4: Correlation Coefficient of Business reactions to cyber threats.....	78

List of Figures

Figure 1.1: History of cyber security	3
Figure 4.1: Bar Graph of Job Description.....	53
Figure 4.2: Bar Graph of Age of respondents	54
Figure 4.3: Bar Graph of individual Cyber security Threats awareness	57
Figure 4.4 Bar graph of IS Security plan.....	58
Figure 4.5: Bar graph of budgetary allocation	59
Figure 4.6: Bar graph of rate of Cyber-Space Security implementation.....	60
Figure 4.7: Bar graph of Presence of cyber security strategies within the organization	61
Figure 4.8: Bar Graph of individual Cyber security consistency with environmental Demands.....	62
Figure 4.9: Bar Graph of individual Cyber security consistency with CCK Expectations.....	63
Figure 4.1.0: Bar graph of composition of information Security Team	66
Figure 4.1.1: Bar Graph of Participation of Top Management in Information Security	67

List of Abbreviations

ATCON-Association of Cybercafé and Telecentres Owners

B2B-Business to business

CBK-Central Bank of Kenya

CCK- Communication Commission of Kenya

CISA- Certified information systems auditor

CMA-Capital Markets Authority

COBIT- Control Objectives for Information and Related Technology

CSIRT-Computer Security Incidence Response Team

DoS-Denial of Service

EAC- East Africa Community

EEI- Edison Electrical Institute

E.g. - Example

Et al.- and company

ICPAK- Institute of Certified Public Accountants of Kenya

IEC- International Electrotechnical Commission

INTERPOL- International Police

IS-Information System

ISO- International Organization for Standardization

ISP- Internet Service Providers

IT –Information Technology

ITU-International Telecommunication Union

KCA-Kenya Communications (Amendment) Act

KENIC-Kenya Network Information Center

KTCIP-Kenya Transparency and Communications Infrastructure Project

MCSK-Music Copyright Society of Kenya

NIST-National Institute of Science and Technology

NPKI- National Public Key Infrastructure

OECD-Organisation for Economic Co-operation and Development

PIN- Personal Identification Number

PwC- Price Waterhouse Coopers

UN- United Nations

US-United States

Acknowledgement

This thesis has been accomplished with encouragement, support and contribution from several people to whom I will forever be indebted.

I owe special thanks to my family and friends who have supported me and cheered me on even when studies were taking a toll on me.

I appreciate my supervisor, Dr Vincent Omwenga, for his patience, guidance and insight, throughout this research project. He has offered me great assistance and direction that went a long way in finalizing this research proposal.

But above all to Almighty God for His overwhelming grace and mercy which have seen me through this programme every step of the way.

Dedication

This is dedicated to my loving family and friends.

CHAPTER ONE

INTRODUCTION

1.1 Background

The International Telecommunication Union (ITU) (2012) defines security as any measures taken to minimize the vulnerabilities of assets and resources. The Security of assets that have been described to include a general support system, equipment, critical system, high strategic program, physical plant, personnel, major application, or a logically related group of systems, (National Institute of Standards and Technology-NIST, 2011) is critical for the efficient operation of an organization. Security also involves the minimization of any vulnerability that could be exploited to infringe a system or the information it contains (Stallings, 2006).

Various aspects of security include: web security, wireless security, network security, information security, computer security and cyber security. This research is focussed on cyber security which ITU (2012) defines as a collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and the user's assets. Cyber security is applied in a cyber environment which includes connected computing devices, telecommunication systems, personnel, services, infrastructure and applications.

Cyber security has been considered to be a fundamental aspect of any organization. Organizations therefore spell out their security guidelines in their information security policy document for use by the whole firm, (Hong, Ching & Tang, 2003; Champlain, 2003; CISA, 2012; Montesino, Fenz & Baluja, 2012). They consider the Information System (IS) security document as a framework for the organization from which all other IS security related controls could be derived.

1.1.1 Brief History of Cyber Security Threats and Cyber Security

Korsell and Krister (2001); D'Ovidio (2007); Sherstobitoff (2008) note that cyber criminals have existed from the 19th century, exploiting the various technological inventions in information, communications and technology over time. D'Ovidio (2007) points out that as with the telegraph, telephone, computers and related networking technologies, the internet has created new frontiers for crime and this has grown in sophistication with the improvements in the above technologies. A summary of how the cyber security crime has then metamorphosed over the years is as tabulated below.

Table 1.1: History of cyber crime

1986-1995	1995-2000	2000-2007	2007 and beyond
-Local area networks(LAN)	-Internet era	-Broadband prevalent	-Peer-to-peer
-First PC virus	-Macro viruses	-Spyware, spam,	-Social engineering
-Boot sector viruses	-Script viruses	phishing	-Application attacks
-Result in system or user havoc	-Result in system or user havoc	-Botnets	-Financial motivation
-Slow propagation	-Faster propagation	-Rootkits	-Targeted attacks
16-bit DOS	32-bit Windows	-Financial motivation	64-bit Windows
		-Internet-wide impact	-State-sponsored cyber terrorism
		32-bit Windows	-Mobile device attacks

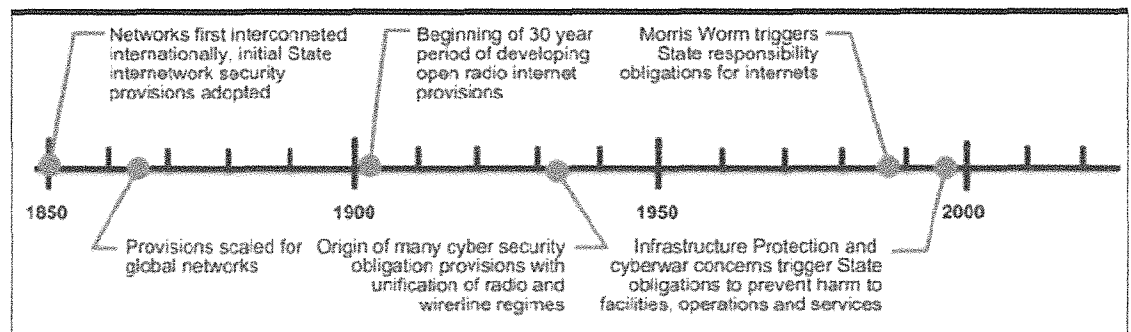
Source: VanDerwerken &Ubell, (2011)

Table 1.1 above shows in brief the stages through which cyber security crimes have gone through over the decades. In earlier years, users relied on local area network (LAN), they advanced to the use of broadband networks and in modern day peer-to-peer systems are being widely adopted. Indeed the degree of sophistication of cyber threats has been heightened to greater levels especially with the invention of the internet. Mobile technology has propelled the existing cyber security threats as modern day mobile phones can access the internet and thus can easily be used to

perpetrate an attack (ITU, 2012). Further improvements and inventions in technology are bound to increase the numbers and magnitude of cyber criminals' activities in cyber space especially with the upcoming social engineering facilities.

The processes and products of IT security has been significantly influenced by the increase in cyber criminals' activities over time (Rutkowski, 2011). Figure 1.1 below is a summary of the historical timelines - dated as far back as 18th century to the 20th century- of cyber security international law provisions.

Figure 1.1: History of cyber security



Source: Rutkowski (2011)

From figure 1.1 above, it can be seen that cyber security attracted the attention of stakeholders from as early as 1850. In those times, the Chinese, Egyptian, and Roman civilizations were seen to be the pioneers in the securing and assurance of communications (Rutowski, 2011). The rest of the countries followed suite and with further convergence of various technologies, i.e. radio, wire line, radio internet, computers and more recently mobile phones, the need for collaboration amongst countries has arisen. This will assist in securing the cyber environment.

According to Saini, Rao and Panda (2012), the current cyber environment is faced by various unprecedented cyber security challenges. Some of the challenges are brought about by the ubiquity of IT and the significant growth in popularity of e-commerce (Hong, et al, 2003). Past research has forwarded suggestions of security countermeasures which could be implemented by an organization such as IT

security policies, application of tools and implementation of a rigorous training program. These, according to Lee and Lee (2002), are based on the General Deterrence Theory, (GDT). This theory suggests that when an institution puts in place cyber security measures that threaten cyber criminals, its cyber security issues will have been addressed. This is quite optimistic as Lee and Lee (2002) note that the cyber security prevalence rate continues to be on the rise contradicting the GDT.

Li (2006) remarks that the high prevalence rate of cyber security attacks reflects on the vulnerability of information systems and shows how far the offensive technology utilized by cyber criminals outpaces the defensive technology utilized by organizations and other stakeholders. A keen look into cyber security by various stakeholders - for example the government, Internet Service Providers (ISPs), business communities, international blocs - would be a great milestone in solving cyber-security concerns.

1.1.2 Business in a Cyber Environment in Kenya

Businesses in Kenya are operating in a relatively stable political environment according to the Kenya Business Environment report (2005). The political environment has an effect on cyber security as it sets the legal tone of a nation. For instance, The Kenya Communications Amendment Act of 1998 shows the Kenya government's initiative to secure the cyber environment that has been marred by diverse challenges over the years.

The Kenya Business Environment report (2005) also defines the Kenya business environment as being well over-regulated. Depending on the industry that one operates in, a regulatory body is often seen to exist to streamline the operations of businesses in a particular sector. For example, the Communications Commission of Kenya (CCK) is the regulatory body in the telecommunications sector, the Institute of Certified Public Accountants of Kenya (ICPAK) regulates the members of the accountancy profession; the Capital Markets Authority (CMA) is the regulatory body for companies listed on the Nairobi Securities Exchange market etc. Regulators offer guidance to and supervision of various registered entities. For

example, a CMA management supervision internal control report dated May 2012 required its members to maintain security controls to ensure the organizations' assets and clients' assets were safeguarded. This extended to cyber security controls as in the recent past, organizations across the sectors have adopted technology in every aspect of their operations. Furthermore, in modern day society, information has been rated as the most valuable commodity, (Korsell& Krister, 2001). Thus it should be secured accordingly.

Much is still to be done to say that cyberspace is secure enough for the well being of all the stakeholders, as absence of security could impede a business' participation in online trade (Ng'ang'a, 2009; ITU, 2012). All parties involved have a responsibility in mitigating cyber security threats, with more emphasis being placed on the responsibility of the end user, remark Rudasill and Moyer (2004).

1.1.3 Various aspects on cyber security

Li (2006) discusses the various schools of thought that attempt to describe the cyber security concept. These include cyber security as an externality, as a private good or as a public good.

a) Cyber security as an Externality

Eeten and Bauer (2008) describe externalities as forms of market failures that create a variance between the social and private costs of production. Market failures often occur as a result of decision makers having incomplete information. Presence of externalities leaves organizations at a less than expected socially desirable security level. There are three externality situations that could arise:

1) *No Externality exists*-This is a case which is very rare as this situation describes a market that operates at perfect position. It occurs where a market player has accurately assessed both the private and social costs and has borne them accordingly. The market player in this case has assessed cyber security risks, has taken into account all the expenses of protecting against these cyber security threats

and has implemented the necessary mechanisms to absorb them, (Eeten & Bauer, 2008; OECD, 2009).

2) Externalities that are borne by certain persons in the system

This is a scenario that arises where a market player takes into account social costs i.e. cyber security risks in his production but, due to inherent market-failures, the decision settled on differs from the socially efficient level, (Eeten & Bauer, 2008). The variation from the social efficient level may arise due to the producers' self interest of profit maximization, a lack of sufficient finances to reach the desirable social optimum, a lack of inducement to absorb costs placed on others or a lack of the required know-how to deal with cyber security risks. Kshetri (2010) remarks that firms that adopt internet technologies with little regard to the holistic costs and efforts needed to maintain those infrastructures produce negative externalities.

For instance, most financial service providers compensate clients for any loss they suffer in case of an instance of online fraud. They absorb the externalities of their customers' sub-optimal security investments, because not doing so would leave them incurring higher costs, as they may experience blacklisting and possible reputation effects, (Eeten & Bauer, 2008; Kshetri, 2010).

3) Externalities that are borne by persons who cannot manage them or by society at large.

Market players may not fully comprehend the externalities they produce for other people thus such externalities will inevitably be borne by all the stakeholders, (ITU, 2011). For instance, the slow growth of e-commerce, the cost of cyber crime activities, and the cost of law enforcement associated with these activities, amongst others.

b) Cyber security as a Private Good

According to Li (2006), information infrastructure is a unique and critical infrastructure-those assets and systems vital to national security, public health or economic need, e.g. energy, public transport, railway system-as it is mainly owned

by the private sector and it is the backbone of many of the above critical infrastructures. As such, Smith and Rupp (2002); Li (2006); Jones (2007); Hans et al. (2010) argue that since information infrastructure is a private good, it follows that cyber security is a private good, mainly in the hands of private persons.

c) Cyber Security as a Public Good

Li (2006); ITU (2011) defines a public good as one where its consumption by one party does not limit the amount accessible for others to consume (non-rival consumption). Public good, is usually confronted with the problem of under provision when put in the private market. Li (2006) views the claim that a government has no role to play in cyber security as being over sceptical and unrealistic. In concurrence, an Ernst and Young Global Information Security survey conducted in 2008 showed that at least 61% of respondents believed the government had a central role to play in fighting cyber crime.

On the same vein, a report by McConnel International (2000) emphasized the important role of the government in putting in place legal procedures of handling the cyber-criminals. There are nations where the rule of law is not well enforced or worse yet it is not in existence, such will be less equipped to participate in the e-economy, (McConnel, 2000; Ng'ang'a, 2009).

Ability of countries to enforce various cyber security laws differs in relation to their government structures, resources, IT capabilities etc. Cole et al. (2008) view African nations as facing much greater socio-economic challenges, such as acute poverty, hunger, AIDS, malaria and many others and thus their governments cannot be expected to focus much on cyber security. In this case, the onus of cyber security will naturally be left in the hands of private businesses.

To wrap this debate up, Sund (2007); EEI (2010); Warfield (2012) suggest that the best of both worlds could be taken so that a well-practiced, public-private partnership which utilizes all stakeholders' expertise could be adopted in the fight against cyber security threats. Broadhurst (2006); Ng'ang'a (2009) reckon that emergence of sophisticated cyber security threats necessitates the need for the

public and private sector to work together to fight the menace. This standpoint seems more fruitful as this cyber security war is a multifaceted beast that requires pulling of resources and expertise from the various stakeholders.

1.1.4 Cyber security in Kenya

A survey by Price waterhouse Coopers (PwC) in 2011 brought to light the difficulties that exist in assessing cybercrime risks. Their report further explained the difficulty in cyber risk assessment; as one would ask, when does one report that a crime has occurred? What costs should one include in estimating losses? Does one consider only proven losses through fraud or also consider non-financial costs like reputation damage? How does one measure such if they are to be included too?

These show that establishing the exact cyber security situation for any entity could be quite a daunting task. However, the following estimates could be relied upon to give an overview of cyber security climate in Kenya.

1.1.4.1 Cybercrime prevalence in Kenya

Magutu, Ondimu and Ipu (2011) noted that Kenya had not yet drawn the attention of highly refined form of cyber crime mainly due its slow internet connectivity which was only accessible in selected towns. The coming on of high internet speed connectivity has attracted both domestic and international cyber criminals who were in the past dissuaded by the high levels of effort and time that was required to break into Kenyan websites by means of slower connections (Ajala, 2007). Magutu et al, (2011) observes that Nairobi was gradually being renowned as a regional nucleus for internet connectivity and this is largely due to affordability and reliability of internet connectivity as a consequence of the acquisition of the fibre optic cable.

Kshetri (2010) points out that Kenya suffered from about 800 bot attacks per day back in July 2009 and the numbers are anticipated to increase exponentially to about 50,000 bot attacks per day upon the going live of the fibre connectivity. More recently, forensic experts reported that cyber crimes have cost the Kenyan economy

about Ksh.3 billion annually and the numbers are expected to grow, (Ng'etich, 2012).

The increased numbers of cyber crimes could indeed be realized as Africa has outpaced the rest of the world with the significant increase in online users (Kshteri, 2010). This is due to the boost accessibility of broadband connections and the reduction in subscription fees (Olowu, 2009). In 2012, CCK estimated the number of internet users to have reached 13.5 million in the quarter to September from 12.1 million users in the previous quarter, (CCK, 2013). Moreover, Grabosky and Smith (2001); Atkinson, Johnson and Phippen (2007) note that in modern day, access to the internet is further extended to mobile devices which has reported global unprecedented growth in recent years.

A recent World Bank report showed that approximately three-quarters of the world's inhabitants had access to mobile phones, (World Bank, 2012). It further reported of the worldwide subscribers in 2012 as being 6 billion yet in 2000 the figure had been less than 1 billion. Kenya has not lagged behind as the CCK report released on January 2013, showed a bump in subscribers numbers which grew to 30.4 million, pushing mobile telephony penetration to 77.2 per cent up from 75 per cent in the quarter to June 2012, (CCK, 2013).

Remarkably, in the 12 months period to January 2013, Kenyans transacted almost double the country's 2012/2013 budget in electronic money transfers and payments, (CBK, 2013). Of this amounts, mobile money was recorded as being the most popular mode of transaction accounting for 59% of the total values, (Mumo, 2013). Africa and more specifically Kenya is indeed moving fast towards being a highly technological nation with a lot of convergences being seen (Olowu, 2009; Magutu et al., 2011). As social media, mobile devices and the cloud become popular in modern day, technology adoption is seen to outpace security, (PwC, 2013). Unfortunately, these convergences of computer and mobile phone technologies have created unmatched vulnerabilities (Grabosky & Smith (2001). Recognizing these vulnerabilities, and implementing the most effective countermeasures, will be a daunting task to the various users, (Salifu, 2008; Olowu, 2009).

1.1.4.2 Cyber security measures adopted in Kenya

Kshetri (2010) recognizes that countries differed in their extent of preparedness in terms of having the necessary regulatory bodies to manage cyber security threats. Kenya took a bold step in 1998 and through an Act of parliament passed the Kenya Communication Act (KCA) to deal with issues surrounding Information and Communication Technology (ICT). Akuta, Ong'oa and Jones (2011) point out that the KCA 1998 did not address the specific issues concerning cybercrime satisfactorily. Consequently, it was amended twice in 2009 to accommodate the several changes that had taken place in the cyber environment. KCA thereafter was at times referred to as E-transactions Act of 2009.

Part VI A, section 83 of the KCA (2009) describes the commission's efforts in relation to providing a cyber-secure environment with an aim of facilitating e-commerce. From section 83 C sub-section (a) to section 83C sub-section (f) the Act stipulates the various functions the commission intend to perform in fostering security for the cyber users. For instance, section 83C (d) the commission lays down its intent to foster the growth of e-commerce through the use of electronic signatures (e-signatures) which will improve the authenticity and integrity of all communications via electronic medium.

The various cyber security threats are outlined from section 83-U to section 84-I with their matching penalties and fines in case where any of the aforementioned crimes are committed. Examples of cyber related crimes under this Act include: unauthorized disclosure of passwords, unauthorized access to protected systems, unauthorized modification of computer material, illegal re-programming of mobile telephone etc.

Sections 106 A and 106 B mentions the admissibility of electronic records in court subject to meeting certain laid down rules. This would assist the law enforcers to offer electronic records for a forensic investigation relating to the cybercrime committed.

Olowu (2009); Ng'ang'a (2009); Kshetri (2010) point out that despite several developing economies having enacted laws to deal with cyber-crime, enforcement mechanisms are yet to be effected. They further note that developing countries lack judges, lawyers and other law enforcement personnel who understand cyber-crime i.e. awareness is generally seen to be low among the law enforcement community. Akuta et al. (2011) recognize attempts by the government to correct this and report that in 2009, 18 Kenyan police officers were sponsored to receive a four months special training in the United States on handling the 'new' crime and the handling of certain specialized tools to trap criminals; meanwhile a retraining of other of the Cyber Crime Unit by their colleagues who had been trained in the US was going on.

Other steps to beef up cyber security include an establishment of a Computer Security Incidence Response Team (CSIRT) by Kenya Network Information Center (KENIC) which works under the auspices of the Ministry of Information and Communication and the Kenya Police (Akuta et al., 2011). This response team, according to Akuta et al., (2011) works at communicating computer and network related security threats and vulnerabilities to the local internet communities. CSIRT will also be involved in incident reporting, incident analysis, incident response and coordination, incident resolution amongst others.

Moreover, a department of Criminal Investigation, in the regular force, was created to investigate and prosecute cyber criminal activities (Akuta et al., 2011). Remarkably, Kshetri (2010) points out that by 2006 Kenya was in the advanced stages of putting up a cyber-crime laboratory, which the police in the East African region could greatly utilize.

Futhermore, a move in fighting cyber security threats was recorded recently where Internet Solution Kenya and Symantec Corps were seen to enter into a partnership and launched security cloud based services that would see security marketed in the East African Region, (Njihia, 2012).

Moreover, in an attempt to secure the online business environment, the National Public Key Infrastructure (NPKI) was initiated by the Kenya government in March

2013. The Ksh. 391 million project is to be undertaken within the framework of the Kenya Transparency and Communications Infrastructure (KTCIP) project with an aim of issuing digital signatures and protect parties involved in e-transactions, (Mumo, 2013).

Much is yet to be done still as cyber security threats' inventions seem to outpace cyber security counter measures, as Kshetri (2010) reports, as late as 2010 sixty per cent of Kenyan banks were still found to have insecure systems. More recently, in 2013, local banking sector had reported to have lost billions of shillings to fraudsters, (Mumo, 2013).

1.2 Theories in cyber security

With the rapid adoption of ICT many organizations have been seen to suffer from unprecedented security issues and challenges. Despite this growing demand for cyber security tools from users in all spheres, there still lacks a theoretical framework for information security management, (Hong et al., 2003).

A review of cyber security literature reveals the following important information security management theories that are widely used in the discussion surrounding cyber security: contingency theory, risk management theory, management systems theory, auditing and control theory, security policy theory, (Hong et al., 2003).

Social criminology theories could also assist in explaining the cyber security phenomenon. A select of the social criminology theories that describe the cyber security agenda include: Social Bond Theory (SBT), General Deterrence Theory (GDT), Theory of planned Behaviour, (TPB), Environmental Criminology Theory (ECT), Routine Activity Theory (RAT), Rational Choice Perspective (RCP) and the Social Learning Theory (SLT).

According to Schuessler (2009), GDT emanated from criminology and it majorly examined deterrence, prevention, detection, and the use of remedies to influence cyber security rates. He goes on to rate GDT as one of 12 top up to date criminology theories. GDT has been the base of several cyber security studies in the past, (Lee&

Lee, 2002; Willison, 2006). Lee and Lee (2002) report that GDT has been applied in the ICT sector over the past 15 years. They cite Straub (1990), Straub and Nance (1990), Goodhue and Straub (1991), Harrington (1996), Straub and Welke (1998) as some of the scholars who have applied the GDT successfully in their studies.

Lee and Lee (2002) acknowledge that GDT has provided background in the computer abuse subject though it has not yielded significant results perhaps due to the fact that the theory is restricted and thus does not touch on all the aspects that affect computer abuse. Willison (2006) notes that GDT is a foundation theory in computer security discussions but beyond the point of deterrence to commit criminal activities, other theories are required to describe the criminal-victim dynamics.

1.3 Statement of the problem

Kshetri (2010) notes that cybercrime footprints are getting bigger and bigger in developing economies. This is echoed by PwC (2011) who report that over the past ten years, their survey revealed that barely anyone was familiar with what cybercrime was. However their 2011 report positioned it as one of the top four economic crimes – just behind asset misappropriation, accounting fraud, and bribery and corruption.

Further, Kshetri (2010); PwC (2011) note that businesses and consumers alike in developing countries have suffered under both local and international cybercrimes. The consequence of this scenario is that businesses do not grow as would be desirable and investment opportunities will be curtailed as the business environment will be regarded as inhospitable (McConnell, 2000). Kshetri (2010) indicates that special attention should be given to developing countries as cyber security is indeed a threat to development of these economies.

To address some of the concerns associated with cyber security, the social identity theory has been applied by Kshetri, (2010) in his research. Social Identity Theory was developed by Tajfel and Turner in 1979 in an attempt to establish the minimal conditions that would lead members of one group to discriminate in favour of the

in-group to which they belonged and against another out-group. Kshetri, (2010) showed that as more people and firms become victims of cybercrime and thus belong to the in-group of cyber-crime victims, the perceived social stigma associated with becoming a cyber-crime victim may reduce (favouritism amongst in-group members) and the prejudice or stereotyping associated with cyber-criminals(out-group members) may increase.

Magutu et al. (2011) report of research on cyber security threats being in its infancy, and this research aimed at contributing to the existing Kenyan literature on the subject. It will aim at establishing the reaction of in-group members (businesses) to the activities of the out-group members (cyber criminals). The study will specifically seek to analyze the various cyber security threats' characteristics, to determine the awareness levels of the in-group members in regard to the out-group members' tactics and the overall reaction of the business society to out-group members' activities, i.e. cyber security threats.

1.4 Research objectives

The study aimed to establish the reaction of Kenyan businesses to cyber security threats, as guided by the following specific objectives:

- i) To analyze cyber security threats' characteristics
- ii) To establish level of awareness of cyber security threats
- iii) To investigate on the manifestation of cyber security threats
- iv) To analyze the business' reaction to cyber security threats

1.5 Research questions

- i) What are the characteristics of cyber security threats?
- ii) What is the cyber security level of awareness among users?
- iii) How do cyber threats manifest themselves in a business environment?
- iv) How have businesses reacted to cyber security threats?

1.6 Significance of the study

The study is important to the following persons:

Software manufacturers-the research findings will show how various cyber security threats are manifested. The software manufacturers will use this to better package their security products for the Kenyan market.

Scholars and academicians-The research will extend the existing knowledge in cyber security threats' awareness levels, manifestations and preparedness of business community.

The Kenya Government-The research findings shall offer guidance to the Kenya government in the formulation of appropriate policies that aim at countering the cyber security threats' menace.

Law community-lawyers and judges will be alerted to recommend new and upgrade other old laws that would then assist in combating the cyber security crimes.

The business community-investors would be keen to know the level of security of Kenya businesses so as to make decisions as regards investment and engagement in e-commerce.

Insurance companies would want to know how businesses perceive this 'new' risk and whether an insurance product of this nature would get market.

Higher education institutions would be keen to know the education needs in the market so as to introduce courses in this area e.g. computer forensic studies.

Bhattacharya (2011) notes that results of such a study could be potentially useful to businesses which are often so dedicated on achieving high growth and profitability but pay little attention to critical details of IS security. Businesses will further get to gauge their preparedness level and better position themselves to secure their network systems.

1.7 Justification for the study

Previously, the reaction of Kenya business to cyber security threats had not yet been established. Thus, this study sought to fill this gap by establishing the cyber security threats' awareness levels and the business' overall reaction to cyber security threats.

1.8 Scope of the study

The study focused on the responses of businesses to cyber security threats in Kenya. It was carried out within various large organizations operating in the different sectors in the Nairobi metropolitan region. The study targeted the IT staff and internal auditors in those firms. The variables under study were: cyber threats' characteristics, cyber security awareness levels, cyber security threats manifestation and business reactions to those threats.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

Chapter two discusses the literature on cyber security threats. Literature review is essential to the scholarly background required for a subject in any research that is being undertaken, (Kabiru& Njenga, 2009). The literature reviewed for this study narrowed on cyber security threats' characteristics, cyber security threats manifestation and reaction of businesses to these cyber security threats.

Hall, Sarkani and Mazzuchi (2011), observe that in recent times, organizations have been urged by national and international regulators to give cyber security due attention. In addition, Broadhurst (2006) points out that cyber security has become more challenging now due to the increase in sophistication of cyber security threats.

In dealing with the increased sophistication of cyber security threats, Smith and Rupp (2002); Abu-Musa (2010); Hall et al. (2011), recommend the implementation of proactive and non-reactionary approaches which should in the long-run, get to earn a competitive edge, improve efficiency, enhance reputation and assurance from other external stakeholders. The implementation of proactive cyber security approaches is dependent on the factors explained under section 2.2.

2.2: Factors influencing Organization's cyber security practice

The absence or presence of cyber security practices in diverse business sectors is dependent on certain key factors:

2.2.1 Costs versus benefits

According to Bishop (2002); Trim (2005); OECD (2009), an organization should be in a position to consider the various risks their assets are likely to face and the likelihood of their occurrence and compare this with the impact if they were to occur so as to establish the amount of investment they would put in securing those systems. From such security analysis, an organization may either adopt an active or

reactionary approach to cyber security. Bhattacharya (2011) notes that firms may be drawn to passive and reactionary approach to cyber security risks and threats as it may seem to be economical and cost-effective. However this approach could be disastrous to the business upon the realization of a cyber attack.

Anita (2000) further points out that several organizations had adopted a reactionary approach due to their inability to calculate the Return on Investment (ROI) in cyber security. Anita suggests the various costs that would arise following a breach of cyber security and Abu-Musa (2010), forwards the various benefits to an organization for implementing effective IS Security measures. These are summarized in the following table:

Table 2.1: Cost versus benefit

Costs of realized Cyber security threats to the business	Benefits to the business of putting in place effective cyber security measures
- lost business, due to unavailability of the breached information resources - lost productivity of the non-IT staff, who would be paralyzed and would have to work in a degraded mode, while the IT staff tries to contain and repair the breach - labour and material costs associated with the IT staff's detection, analysis and repair of the breached resources - legal costs associated with the collection of forensic evidence and the prosecution of an attacker - public relations consulting costs, to prepare statements for the press, and answer aggrieved customer questions - increases in insurance premiums (if insured) - costs of defending the company in any liability suits resulting from the breach of a contract to deliver assured information and services - cost of being blacklisted (where applicable)	- an increase in share value for organizations that practice good governance - increased predictability and reduced uncertainty of business operations by lowering information security related risks to definable and acceptable levels - protection from the increasing potential for civil or legal liability as a result of information inaccuracy or the absence of due care - a firm foundation for efficient and effective risk management process - improvement, and rapid incident response related to securing information - a level of assurance that critical decisions are not based on faulty information; - accountability for safeguarding information during critical business activities, such as mergers and acquisitions, business process recovery, and regulatory response.

Source: Anita (2000) and Abu-Musa (2010)

From table 2.1 above, the benefits arising from implementing a cyber security strategy clearly out-do the costs. However, Eeten and Bauer (2008) note that the success of several cyber security measures remains doubtful and in dispute. Moreover, Abu-Musa (2010) notes that despite the increase in spending on security over time, the inability of security measures to deal with various cyber security threats e.g. identity theft, loss of management's sensitive information and various other criminal acts continued to persist.

Some other opponents of IS Security include: Volonino and Robinson (2004), Ajala (2007); Eeten and Bauer (2008), who note that IS Security slows down business processes, has too much cash requirement and requires too high staffing which may not be economical in the long run. Further, security measures may have negative effects on innovation, productivity and may inconvenience the end user.

The onus is on management to weigh the costs against the benefits and choose an optimal security level on which to operate on.

2.2.2 Organization's Dependence on IT

The criticality of IT to an organization is well assessed by McFarlan's grid which helps organizations assess their current and future dependence on Information Systems.

Nolan and McFarlan, (2005) describe the first half of the grid as one that shows the degree to which the firm relies on cost-effective, secure, uninterrupted systems (Defensive IT) and the second half explains the degree to which the firm relies on IT to provide new value-added products to their customers that would yield competitive advantage (Offensive IT). Depending on the quadrant which the organization's IT system reliance falls, the management should attach the corresponding attention on cyber security matters. Security would either be a routine issue handled at the IT level or a crucial matter handled at the board level.

Table 2.2: McFarlan's Grid

Low to high need of reliable IT	DEFENSIVE	OFFENSIVE
	Factory Mode - Applications that are critical to sustaining existing business -slight disruption causes much impair to the business operations. -delay in response time has consequences for both internal and external customers - most core activities are online -systems mostly works as maintenance - system work provides little differentiation or competitive edge	Strategic Mode -The organization relies on IT for smooth running of the business and similarly IT could enable the company enjoy future competitive advantage -if systems fail momentarily, there is an immediate effect on business -delay in response time has consequences for both internal and external customers -new systems have potential to transform business operations -upcoming systems have potentials of reducing costs -new systems have potential to yield competitive advantage to the Company
	Support Mode -Applications that assist in simple performance of day to day tasks but are not critical to the business -perpetual service interruptions have little effect to business -systems mainly perform maintenance functions -limited future opportunities in technological developments	Turnaround Mode -new systems promise significant transformations in business operations -IT has potential of gaining the company competitive advantage in the future -IT has potential to reduce business costs in the future
	Low to high need of information	

Source: ACCA, (2009); Nolan & McFarlan, (2005)

2.2.3 Nature of sector

Organizations in different industries are seen to have divergent security requirements primarily on the basis of their unique characteristics, (Chang & Yeh, 2006). They further note that these organizations in different sectors call for different levels of information confidentiality, availability and integrity.

Deloitte, (2004); Chang and Yeh (2006); Bronk, Monk and Villasenor (2012); note that banking or financial businesses seem to attract the highest cyber security risks as they are in a highly computerized and information-intensive sector. As banking and financial institutions' IT system reliance falls on the Strategic mode of the

McFarlan's grid, (see table 2.2 above), Monk and Villasenor (2012) note that they have also dedicated significant attention to cyber security. They recommend such firms to consider risk transference approaches in combating IS security threats. By contrast, manufacturing organizations' IT system reliance falls on the Support mode of the McFarlan's grid, (see table 2.2 above) and thus have less strategic IS applications (Jenkins, 2001). IS security threat alleviation strategy of this sector would be one that emphasizes a focuses on the application of fundamental countermeasures, (Monk & Villasenor, 2012).

2.2.4 Diverse User Needs

According to Eeten and Bauer (2008), different IT users need to appreciate that business models vary widely in the different factions of the multifaceted ecosystem surrounding IS— from end users, to internet service providers, to public service organizations, to software manufacturers. The above actors face cyber security threats differently, and experience different costs and benefits in association with the various courses of action. Thus an organization need not ape another firm's IS Security practices blindly; a consideration of the disparity of various business models should be made.

2.2.5 Size of the Business

An organization is described as large or small on the basis of number of employees, turnover, market share that they control and value of their assets. Using turnover as the parameter, Kenya Revenue Authority (KRA) describes a large company as one that has a turnover of more than Ksh. 750 million per annum. On the other hand, those with annual turnover of less than Ksh. 750 million are classified as medium and small sized.

According to Jenkins (2001), Ernst and Young (2008), a bulk of large firms seem to have in place detailed security policies, procedures and major security technologies. Typically, in these large organizations, a steering committee exists, they implore the services of professional systems specialists and management is seen to give considerable attention to security.

On the contrary, Bhattacharya (2011) observes that due to resource, size and skill constraints, small businesses are habitually seen to be unequipped to fight the emergence of cyber security threats. Present day research shows that the information systems of small businesses in the USA are susceptible to cyber security threats, (Bhattacharya, 2011). The problem is that small businesses seem aloof and distanced towards cyber security issues. This aloofness, usually results to sluggish or incorrectly implemented IS security countermeasures, which worsens their vulnerability to cyber security threats, (ITU, 2012).

2.2.6 Vulnerability of Specific Business Sectors

Fletcher (2007); Kshetri (2010) describe some businesses as being more vulnerable than others based on their attractiveness to criminals. Financial sectors, he notes, were the early users of IT and thus attracted computer fraudsters early too. He explains the attraction as having been brought about by the money aspect that typifies the financial sector. According to Sund (2007); Fletcher (2007), criminals follow opportunities; and thus fraud in relation to the e-finance sector right away succeeded the initiation of e-business. Further on, Bhattacharya (2011) discusses cybercriminals as being increasingly focused on various types of fraud for motives of financial gain.

Therefore, companies that adopt e-finance, e-banking and e-commerce in their day to day transactions are deemed to be more vulnerable than those that do not and should thus invest in IS Security accordingly. As financial sector is seen to have the highest reputational and operational risk, it should lead the way in instituting controls, (Deloitte, 2011).

2.2.7 Existence of Legislations

According to McCrohan (2003), a need for all companies that operate within a business to business (B2B) environment to maintain basic auditable security standards has arisen. For instance, in the US, a National Security Council hosted a group of key stakeholders to deliberate on the basic security standards that would have to be met for internet-connected companies.

In Kenya, Magutu et al. (2011) note that ISPs are required to meet certain basic security requirements by CCK in order to be allowed to practice. The existence of such standards set by certain recognized bodies, leave the organizations involved with little option but to implement security standards or else suffer certain consequences.

2.2.8 Financial Position

Kshetri (2010) notes that developing economies seem to be deficient in the resources required to bring up institutions to fight cyber security threats. Similarly, the organizations which exude greater financial strength are better placed to implement the various IS security measures as opposed to organizations which seem to be at a weaker financial position. As Montesino, Fenz and Baluja (2012) notes 133 security controls are suggested for implementation by the International Organization for Standardization (ISO). This may prove to be quite a daunting task for financially weak firms. Inadequate resources may thus force some organizations to endure a higher than acceptable risk when implementing IS Security, (Pathak, 2004).

2.2.9 Knowledge

Kshetri (2010) describes third world countries as lacking in skills and knowledge to combat cyber-crime. The implementation of up to date cyber security counter measures is impeded by the lack of information and expertise for several firms.

2.3 Characteristics of cyber security threats

These may include:

2.3.1 Borderless

Smith and Rupp (2002); Korsell and Krister (2001); Fletcher (2007); Salifu (2008); Akuta et al. (2011) describe IT Security threats as being borderless with no clear cut jurisdiction thus cyber attackers and cyber victims are seen to be located anywhere in the world. Jones (2007) describes this aspect of cyber security threats as reverse

proximity which enables cyber criminals, through use of technology, to contact victims across great distances all over the world.

2.3.2 Unobserved Ethical Boundaries

Smith and Rupp (2002) interestingly note that ethical boundaries are not observed in the cyber world as people tend to ignore ethics in the cyber world. For example, one would not consider stealing a protected e-document as theft yet one would not engage in the same in the real world. Cronin (2001) observes that cyber security threats are indeed characterized by ambiguous ethical boundaries which the various cyber criminals exploit.

2.3.3 Difficulty in Establishing Person Responsible

Fletcher (2007) points out that it may sometimes be very difficult to establish the person responsible for certain IS Security threats. For instance, he cites from The Banker (2005) of an American Miami businessman whose account had been illegally accessed by cyber criminals through a key-logging virus, which had infected the victim's computer. As a result, money had been transmitted from his bank account illegally. The defendant claimed their systems were robust and thus denied responsibility for the robbery. The claimant disputed further and argued that the bank was lax as they should have contacted him before effecting the transfer. The questions that followed were: Who is the victim and who is responsible for the IS security attack? These are some of the complexities that surround cyber security threats and attacks.

2.3.4 Difficulty in prosecuting offenders

McCrohan (2003); Brenner (2004); Salifu (2008); Ng'ang'a (2009) note that cyber criminals exploit loopholes in the law as most countries' legislations are yet to fully provide for the various cyber-crimes. Further on, certain countries' laws do not recognize certain cyber crimes. For example, Brenner (2004) points out that in Brazil hacking by itself is not deemed to be a crime while in Kenya it is considered as one. Further difficulty is experienced when gathering the evidence required for proving cyber security crimes (Fletcher, 2007). Brenner (2004) notes that this

challenge is further heightened by the lack of paper trail which would act as evidence.

2.3.5 Threats have a Multiplier Effect

Cronin (2001); Brenner (2004); Broadhurst (2006) discuss cyber security threats as having multiplier effects and scalability. This is easily achieved through use of automation i.e. software tools such as botnets. Brenner (2004); Jones (2007) distinguish cyber-crimes from traditional crimes on this basis of automation. Automation enables a criminal to plant an attack and leave it to multiply itself at very fast rate and with minimal human intervention. This widens the cyber-crime scale as the degree of harm that a person can cause single-handedly in the cyber world, in reality could only be compared to an attack conducted by a whole army.

2.3.6 Low Cost

McCrohan (2003); Broadhurst (2006) ;ITU (2011) describe cyber security threats as requiring low costs of entry as all that one requires is a connected computer and basic technical skills. For instance, a criminal with basic technical skills could easily access an online 'easy to use' manual and 'easy to use' hacking tools which he would then use to commit cyber-related crimes.

2.3.7 Few Reported Cases

Fletcher (2007) describes cyber-crimes as being different from normal crimes where the victims often report upon being attacked. Characteristically, Broadhurst (2006); Olowu (2009); Magutu et al. (2011) note that cyber-crime victims do not report cyber security attacks as in most instances reporting would attract negative publicity. Salifu (2008) detailed that banks and various other firms in the financial sector were seen to be reticent, for fear of the potential damage to their reputations. These aggravate the cyber security matter as the victims do not get to share their experiences which would have gone a long way in curbing cyber security attacks.

2.3.8 Anonymity

According to Brenner (2004); Etsebeth (2007); Sund (2007); Jones (2007); Donato (2009), Dion (2011) cyber space is characterized by anonymity, as a consequence cyber security threats are too characterized by anonymity. This affords the attackers the benefit of security and privacy which catalyzes their criminal activities.

2.4 Manifestation of Cyber Security Threats

A threat to a computing system is a set of conditions that has the likelihood to cause loss or harm, Willison (2006). For an existing threat to materialize, an attack has to take place. An attack is described as an act by an impostor that entails the exploitation of some vulnerability with intent of causing an existing threat to occur, (Amoroso, 1994). The malicious intruder in the above definition deliberately excludes innocent errors that could result into a cyber-security attack. The interplay of cyber security vulnerability, threat and attack has to be well understood by an organization in order to close all possible vulnerabilities that would enable a threat to be exploited and as a result an attack will be experienced in that organization.

An organization would too need an understanding of the various cyber security attackers and their diverse motivational factors as a starting point in fighting cyber security threats.

2.4.1 Types of Cyber Security Attackers:

Some of the types of cyber attackers according to Saini, Rao and Panda (2011) include:

- a) **Crackers:** These persons aim at committing cyber space crimes for fun or with an aim to gratify some antisocial drive.
- b) **Hackers:** These persons forcefully access their targets' computer systems for knowledge sake, to keep up with their peers or simply out of curiosity. Salifu (2008) describes a hacker as young, fairly educated and of middle income families who does not have previous criminal record.

Smith and Rupp (2002) referred to Landreth (1985) as one of the first people to describe hackers. He classified them into five categories: novice, tourist, student, crasher and thief. He describes the novice as the least experienced, the tourist as one who hacked simply for the adventure, the student as one who was bored and decided to excite himself through hacking, the crasher was simply destructive and the thief was one who was out to make profit out of the hacking.

Smith and Rupp (2002); Saini et al. (2011) indicated that hackers were generally motivated by: the desire to learn, the excitement to succeed, the need to gain the admiration of their colleagues, to build a reputation, or gain acceptance as an expert without formal education.

c) **Pranksters:** These persons just go out to trick their targets. They usually do not have the intention to cause any specific or serious harm.

d) **Career criminals:** These persons rely on crime for a source of surviving and are generally characterized as malicious, addicts, irrational and incompetent people.

e) **Cyber terrorists:** There exist different forms of cyber terrorism. In some instances it would be a smart hacker who forcefully accessed a government website, other instances it would be a number of like-minded internet users who collapse a website by overwhelming it.

All the above could be broadly categorized based on intellectual levels, into an elite group, neophytes, and losers and lamers, (Smith & Rupp, (2002). This categorization is focused on more social aspects like education levels, family life etc. He described the elite group, as the word suggests are knowledgeable people who are out to prove themselves as such, the neophytes were similarly knowledgeable but trailed behind the elite group and the losers and lamers who displayed the least intellectual levels.

The types of cyber attackers could also be broadly classified, based on the source of the cyber attack, into internal or external categories.

Internally, employees are considered a major threat to an organization's computer system. Panko (2010) highlights employees as being dangerous for the following reasons; they have extensive knowledge of the systems in place, they have the privileged access to sensitive areas of the organization's database, they are aware of the controls in place and thus know how best to circumvent them, and the organizations they work for seem to trust them. Employees could exploit any of the several cyber security threats possible e.g. they could engage in employee sabotage, which is the destruction of hardware or software or data, or employee hacking which is the intentional access of computer information without authorization, amongst others. Trim (2005) notes that employee hacking is becoming very popular in recent times and thus management should be aware.

Smith and Rupp (2002) describe internal attackers as being selfish, introverted with lots of personal issues. Ironically, they note that minimal studies have been conducted in relation to internal attackers yet they are the most costly and least caught group.

Externally, the organization has several other enemies to look out for. These could be, competitors, ex-employees, professional cyber criminals, organization stakeholders like suppliers, customers etc. Smith and Rupp (2002) described characteristics of an external attacker as predominantly male, single, between 12-30 years, a loner and often seen to come from a dysfunctional family.

The research will focus on the external sources of threats and their manifestations in a business environment.

2.4.2 Cyber Security Threats

As noted under section 2.2.6, cyber criminals are motivated by financial gains majorly thus most cyber security threats are tuned to where the money is, i.e. businesses. Thus the various threats discussed under this section are restricted to only those that are likely to affect businesses across the divide.

Cyber environment is not static but very dynamic instead. Consequently, with each passing day, new threats are released thus the list is not exhaustive. Nonetheless the list extensively captures the various threats experienced by businesses in modern day.

a) Malware

Etsebeth (2007); Pfleeger and Pfleeger (2007) define malware as a software program that is produced with the aim of modifying computer or network systems without the approval of the owner. Examples of malware include: Trojan horse, viruses, hoax, computer worms and spyware.

This malware threats can have very costly damages if they were to occur; for example, 'ILOVEYOU' virus spread rapidly across the world seriously disrupting IT systems globally, (Korsell & Krister, 2001).

b) Cyber Laundering

Keene (2011) observes that virtual environments are indeed proving to be serene environments for cyber criminals to launder money as it is anonymous, cheap and tax-free. ITU (2011) divides the money-laundering phases into three: placement, layering and integration. All these stages could be executed much more easily through internet use.

c) Smurfing

Keene (2011) defines smurfing, also known as structuring, as the executing of financial transactions, such as the depositing of cash in the bank, in a manner that circumvents the requirement by law to maintain certain records that would aid the identification of suspicious financial transactions.

d) Denial of Service

ITU (2011) notes that denial of service attacks aim at saturating capacity of a target's infrastructure so as to interfere with its proper operation. Some examples of high profile sufferers of DoS attacks include Yahoo, eBay, Amazon and CNN.

e) Advance Fee Fraud

Ampratwum (2009) an advance fee fraud is also known as “419”. A “419” is named after the section of the Nigerian Criminal Code prohibiting the practice. While advance fee fraud or “419s” can take a variety of forms, typically, the sender will seek to involve the recipient in a scheme to earn millions of dollars through illegal acts.

According to Salifu (2008) this could be through helping transfer money supposedly stolen from Nigeria or another country by a late dictator, or through taking a cut on a big public works contract. Recipients who are sufficiently greedy and gullible to agree will gradually be asked to make payments of some thousands of dollars to cover fictitious local taxes, spurious regulatory fees or non-existent legal costs (Ampratwum, 2009).

f) Cyber Squatting

ITU (2011) describe cyber-squatting as the illegal process of registering a domain name identical or similar to the trademark of a certain target’s product or company. This would cause harm to an organization as they may have their business being redirected to the attacker’s domain.

g) Encryption

According to Jones (2007), encryption involves the use of algorithms, to encode data into some form that cannot be deciphered by those who do not have the key or password to decrypt it. It can be utilized by both the victim and criminal for diverse reasons. Criminals use the encryption technology to hide their identity from the eyes of the law enforcers making prosecution a challenge.

h) Social Engineering

Benznosov and Beznosova (2007) refer to remarks made by the then Microsoft’s Vice President for the Windows core operating system, who noted that a good percentage of users face IS security issues as a result of falling for social

engineering tactics. This could be seen to be true as ITU (2011) notes that the weakest link in any IS Security system is often the users operating the system. Common social engineering techniques include:

1. **Reverse Social Engineering:** According to CISCO (2005), during a reverse social engineering attack, the naïve user is prompted to ask the criminal for assistance; as the criminal purports to be a person of authority. For instance, the attacker may advertise that he is the appropriate person to fix an IT problem. When he goes to fix it, he requests certain bits of information from the users which he then uses to cause harm.

2. **Phishing:** ITU (2011) defines phishing as the type of crime where a criminal masquerades himself- via email-as a trust worthy person so as to fraudulently acquire certain sensitive information e.g. PINS.

3. **Vishing:** CISCO (2005) notes that in a vishing attack, the attacker exploits voice technology e.g. voice email, VoIP (voice over IP), landline or cellular telephone so as to obtain certain sensitive information like password or PIN from the target.

i) **Data Interference**

ITU (2011) notes that a criminal may interfere with an organization's data flow by deleting, suppressing, altering and restricting access to the data. Lack of access to data may lead to significant reputational and financial damage to the victim organization.

j) **Botnets**

Adomi and Igun (2008) describe "botnet" technology as one that facilitates the control of tens of thousands of PCs. These PCs are used to spread malware or to flood websites with so much traffic such that the sites break down in DoS attacks. Beznosov and Beznosova (2007), note that currently, attackers exploit social engineering aspects in carrying out botnet attacks.

k) System Interference

According to ITU (2011), a business rival may send remote attacks or physical attacks targeted at certain specific systems of an opponent organization. Physical attacks may be difficult to carry out and thus remote attacks are preferred as internet is anonymous and can be accessed from anywhere. Examples of this are computer worms and DoS attacks.

l) Libel and False Information

ITU (2011) discusses the internet as being greatly used to spread misinformation just in the same way it is used to spread information. Defamation, cyber-smearing, publishing of false information and disclosure of secret information are all likelihoods that could easily be exploited via the internet. Cronin (2001) notes that libel and false information have the potential to reach far at high speed, in the process causing frustration, inconvenience, further bruising the reputation and image of the victim's organization.

m) Spam

ITU (2011) describe spam as the emission of unsolicited bulk messages to a certain target. Often the emails would contain certain malicious software which when clicked on, results to infection of the user's computer, (Sund, 2007). They may also be sent with false return addresses which victims will rely on as proof of originality of the spam, (Magutu et al., 2011). This form of attack is well exploited as Sund (2007) reports, spam accounts for about 90 per cent of the e-mail traffic over the internet; thus organizations must invest in the necessary measures to curb this menace.

n) Eavesdropping

Stallings (2008) refers to eavesdropping as an attacker's endeavors to learn the password of the target through observing the target, finding a writing of the password or other approaches which are based on close proximity of the attacker and target. It could also involve the use of keyloggers.

o) Copy-right Piracy

ITU (2011) notes that the switch from analogue to digital technology gave rise to new copyright violations. Current technology enables the duplication of various digital source documents without loss of quality. An organization may be a victim of this crime where their copy-right protected file, songs and software are exchanged largely without their consent. Magutu et al. (2011) point out that this piracy is quite easy to undertake thus its high prevalence.

According to Njihia (2012) Safaricom Limited was recently sued on breach of Music copyright as guided by the Music Copyright Society of Kenya (MCSK). The injured party accused Safaricom Limited on infringing the copy rights on his top song titles. He further accused them of engaging on piracy by reproducing, modifying, mutilating and offering the songs for sale via mobile phones and internet without his consent. The case is still undecided though proof of damage could be a daunting task for the accuser.

p) Malicious Code

Magutu et al. (2011) describe malicious code as a software program created to move from machine to machine with intent to violate the target's IS.

q) Identity Theft

Increased sophistication of identity theft has been reported in the twenty-first century, due to the growth in reliance on electronic data and online identification, (Sund, 2007). ITU (2011) defines identity theft as the criminal act of fraudulently obtaining and using another person's identity. The offender may use physical methods e.g. stealing computer storage devices, or non-physical methods e.g. dumpster diving, mail theft, Google hacking and social engineering techniques, (Sund, 2007; Ng'ang'a, 2009).

r) IP Spoofing

Jones (2007) describes IP Spoofing as one that takes place when a cyber criminal uses certain software to masquerade his Internet Protocol address so that it matches that of a “genuine” site. Thereafter, he deceives innocent users to offer him certain personal sensitive information.

2.5 Effects of Cyber Security Threats

These are the aftermath of realization and actualization of a cyber-security threat. The effects may either be felt immediately or after some while depending on the exact nature of the threat and the organization’s ability to detect an attack. The effects could generally be classified as direct or indirect.

2.5.1 Direct Effects

Etsebeth (2007) notes that all cyber security threats have their main focus being to target either the integrity, confidentiality or availability of the target firm’s IS and its resources. She goes on to classify the impact of the threat on the basis of these three core components of cyber security:

Table 2.3: Direct effects of cyber security threats

Confidentiality	Integrity	Availability
• capturing and forwarding of passwords; • forwarding of personal and confidential files to public forums e.g. twitter; • capturing of credit card numbers and sending them to a third party; • capturing of keystrokes and passwords; • uploading and downloading files; • observing whatever is on the server's screen.	• the modification and overwriting of objects; • corruption of system files and system areas by random or non-random disk writers, • data diddling whereby targeted data files are modified through corrupting of spreadsheet formulas; • corruption of application files and data files by unauthorized file writers; • modification of encryption programs; • changing configurations; • scrambling of system information.	• deletion of files and folders; • renaming or encryption files; • rebooting the computer; • disabling of security systems; • corruption of software or killing program processes; • theft of confidential and financial information; • denial of service attacks.

Source: Etsebeth, (2007)

The above are the overt effects of a cyber security attack. The impact of attacks that target the confidentiality, availability or integrity of systems are felt almost as soon as the attack is finalized although the ease of detection and arrest of the attack is majorly pegged on the deterrent, detective and preventive tools in place in an organization, (Schuessler, 2011).

2.5.2 Indirect Effects

These are usually experienced in the long run and may include:

- Loss of organization's customers;
- Loss of organization's suppliers;
- Loss of a firm's hard earned reputation;

- Loss of an organization's competitive advantage;
- Loss of staff morale;
- Public embarrassment;
- Decrease in profitability and cash flow.

According to Etsebeth (2007) there could be another form of indirect effect where by a user responds inappropriately when faced by a certain cyber security threat for e.g. a user reformatting unnecessarily, causing more damage than the one caused by the direct attack itself.

2.6 Businesses Reactions to Cyber Security

For most firms, IS security is considered as a game that is very difficult to win. The rules keep changing, and cyber attackers are equipping themselves with proficient technological skills that further heighten the risks, (PwC, 2013).

Moreover, Solms and Solms (2004) note that information security governance is a complicated issue with neither silver bullet nor a single "off the shelf" solution. Trim (2005); Ernst and Young, (2008) have indicated that the complexity of the cyber security war creates the need for senior managers to view cyber security in a holistic context. Any business, in a bid to self-protect their assets, should aim at attaining some degree of harmony between technology, people and procedures.

Hence this section discusses the various ways businesses are reacting and invoking the use of countermeasures in fighting this menace.

2.6.1 Cyber-crime Combating Approaches

A major constituent of IS security is a state's capacity to deter, prevent, detect, investigate, and indict cyber criminal activities, (Salifu, 2008). Fletcher (2007) notes that there are five main levels at which regulation takes place on the cyber space, i.e. the ISPs, state-funded public police organizations, the users, state-funded non-police organizations and corporate security organizations.

Salifu (2008) suggests a legal approach which is mainly carried out by the state-funded public and non-public police organizations levels as mentioned above by

Fletcher (2007). Salifu (2008) further suggests an organizational approach which mainly aims to put into effect laws, to encourage cooperation and to alert the public through the founding of committed institutions. A technological approach could be applied too to enable the investigation and effective analysis of cyber crime issues with the assistance of fresh technologies. This approach is applied by all the various stakeholders as discussed by Fletcher (2007).

This research will focus specifically on the combating approaches adopted by users i.e. the organizations. These could be broadly classified into external and internal combating approaches as follows:

2.6.1.1 External Combating Approaches:

Chang and Yeh (2006) discuss that in the public arena, organizations need to participate in the various programs and exercises that are put forward by government agencies in a bid to secure the cyber environment. In Kenya, CSIRT is in existence and it requires organizations to participate in incident reporting and incident analysis.

Information sharing could also be enhanced between the public and private sectors where by specific sectors can be matched with specific government agencies that deal in the same business (McCrohan, 2003). For example information and communication industry can be linked with Ministry of Information, banking and finance sector can be matched with Ministry of finance etc.

Organizations should also collude with their competitors in the same industry in a bid to share their experiences as regards cyber security threats (PwC, 2011). As it is, cyber crime victims opt to suffer in silence for various reasons: reputational damage, for lack of evidence or for having little faith in the judicious systems (Fletcher, 2007). Furthermore, Saini et al. (2012) note that the companies' reluctance to report breaches could be due to an organization's top leaderships' embarrassment, apprehension of future similar or worse crimes and fear of exploitation of these attacks by rival firms so as to gain competitive advantage. This

works to the favour of the cyber criminals who thrive under the silence of their cyber crime victims.

2.6.1.2 Internal Combating Approaches:

Given the array of cyber threats, organizations should have cyber security embedded in their culture. To achieve this, the general deterrence theory, (GDT) approaches could be adopted and continuously reviewed in their organizations. As discussed in section 1.2, the GDT distinguishes combating approaches into deterrent, preventive, detective and remedial. The following are the various GDT approaches that could be applied by an organization:

a) Business use of technological approaches

Salifu (2008); Kenee (2011) suggest that technology could be used as a weapon by various users in order to obtain an asymmetric advantage over the criminals. Some of the technological approaches that could be adopted include:

1) Anti-spam Filter Technology

Cheswick, Bellovin and Rubin (2003); ITU (2011), describe this technology as one that identifies spam using keyword filters or black lists of spammers' IP addresses. This could be employed by management to assist in filtering out spam mails.

2) Anti-piracy

ITU (2011); Montesino et al. (2012), note that players in the entertainment industry have discovered an encryption technology i.e. anti-piracy software which is designed to prevent users from making copies of DVDs and CDs .

3) Anti-jam

Cheswick et al. (2003); NIST (2011) describe anti-jam tools as those countermeasures that work on making certain that all transmitted data can be received regardless of deliberate jamming efforts. An organization would implement this to counter denial of service attacks.

4) Anti-spoof

Mell, Bergeron and Henning (2005); NIST (2011) describe anti-spoof tools as those countermeasures that avert the unauthorized exploitation of legitimate identification and authentication data that attackers make use of to send spoofed emails to innocent persons.

5) Antispyware Software

According to Mell et al. (2005); NIST (2011) an antispyware software program works on the detection of both malware and non-malware types of spyware.

6) Honey pot

According to ITU (2011); CISA (2012) a honey pot is a specially configured server, created to attract and monitor intruders without risk to production systems or data. If the honey pot works as intended, the organization may get to learn of the intruders' tact and seal all the likely loopholes before they are exploited.

7) Data backup systems

Halsall (2005); Montesino et al. (2012) suggest that backup copies of vital information and software should be safely kept and tested frequently. According to Harrington (2005), information could be backed-up in external hard drives, tapes, CD/ DVDs, internet or the organization may outsource the backup function. The management should check for the reliability of the backup media and should ensure to store the backup media away from the original files.

8) Password

ITU (2011); CISA (2012); Montesino et al. (2012), define a password as a computer encrypted series of characters that act as confidential authentication information, usually used to limit access to users who have the right to access certain information. Passwords are widely used across the world as they are relatively cheap and effective in the application of Principle of Least Privilege. According to Amoroso (1994) the Principle of Least Privilege states that users should only be

permitted privileges to perform certain operations for which they have a need. Their need is defined by their job function. A password therefore restricts access to only the privileged users who indeed need to access that information.

9) Anti-virus software

NIST (2011) defines antivirus as a software program that continually offers surveillance to a computer or network so as to spot all sorts of malware and prevent or detect malware incident. CISCO (2005) describes the working of an antivirus software application as one that scans the hard disk and memory of the user's computer. If the application identifies a virus, it alerts the user who then decides how best to handle the virus.

10) Encryption

According to Jones (2007); Montesino et al. (2012), encryption is a valuable technology that users can use to protect their information from unauthorized access. ITU, (2012) views encryption as a valuable tool that if used improperly can interfere with the goals of an organization.

11) User Authentication

Cheswick et al. (2003); ITU (2011) describe authentication as process of proving one's identity. They describe authentication as one that is based on either; something one knows i.e. passwords and PINs, something one has i.e. job cards and other authentication devices or something one is i.e. biological attributes (biometrics).

12) Digital Signatures

According to Champlain (2003); Cheswick et al. (2003); Stallings (2006), digital signature is data affixed to a data unit that facilitate the establishment of the source by the data recipient. The recipient with the digital signature will too be able to establish the integrity of the data unit and thus protect themselves against e-forgery.

Kenya through the NPKI intends to issue digital signatures that are to help secure online transactions, (Mumo, 2013).

13) Firewall

Cheswik et al. (2003); Microsoft (2012) define a firewall as a software program or hardware that works at deterring hackers, viruses and worms that try to get to a targets' computer via the cyber space. Upon the successful installation of a firewall a firm should keep abreast of the various emerging firewall threats and advances so as to ensure the successful performance of the firewall, (Trim, 2005).

14) Patch

According to Jones (2007), patches are extra bits of code created to tackle issue of bugs in software. Patches facilitate extra functionality and tackle security defects within a program. They have however proven to be inadequate due to failure by users to update the patches within the recommended time, (Broadhurst, 2006).

b) Capacity Development

Benznosov and Beznosova (2007); Ernst and Young, (2008); Saini et al. (2012) point out that persons who understand the rigor of the cyber security threat appreciate that the menace cannot be solved with technology only. They point out that the cyber attackers are focusing much attention on the importance of human and social aspects in the cyber crime menace.

The main personnel issues include: training users on their security responsibilities and IS system procedures for reporting incidents. More specifically, users would be trained on what amount to rightful use of IS assets, the cost of wrongful use of IS assets, and professional system auditors would be trained to appraise IS asset handling (Saini et al., 2012). This training would reduce human error and thus cyber space vulnerability (McCrohan, 2003; Deloitte, 2011).

c) Policy and Guidelines Development

According to Hong et al. (2003); Champlain (2003); ITU (2012); Saini et al. (2012), an information security policy provides IS security direction to the management and the rest of the organization. This IS policy should be communicated throughout an organization in a form that is concise, precise, relevant and understandable to the targeted reader. Additionally, the IS security policy should guide the distribution of IS security responsibilities in the organization, (CISA, 2012).

d) Insurance and Risk Transference

Gordon, Gordon and Sohail (2003) advocate for the transference of cyber threats risk to insurance companies. Risk transferring is a measure that aims at shifting a cyber security risk to another firm, such as an insurer.

In reference to section 2.2 of this research, firms that rely much on IS for their strategic positioning could consider this insurance approach in dealing with IS security threats.

e) Business Continuity Management

According to Chang and Yeh (2006), business continuity management is a measure that safeguards critical business processes from the outcome of disasters and it also counters any deliberately planned disruption to normal business activities. Firms should have in place various business continuity plans on standby so that in the likelihood that they suffer a cyber attack, they have a pre-planned exit strategy.

f) Audits

Regular and irregular checks and reviews of the IS security status could assist in lowering the vulnerabilities in the firm's IS, (CISA, 2012; Vroom & Von Solms, 2004).

In summary, for the effective application of the above approaches, Systems Administration on Network and Security Institute (2000); Abu-Musa (2010), describe the various roles to be performed by management, IT staff and employees as follows:

Table 2.4: Organizational Measures

Management	IT employees	Employees
-Management should be in full charge of all security matters -management should have in place an operational security policy document -they should be in recognition of the various organizational information assets -assigning trained personnel to manage security related issues in the organization -recognition of the various cyber security matters that surround them and implementing the various technical and non-technical controls -authorizing proactive long-term security controls with various regular upgrading of the controls - accountability to shareholders -compliance with legal requirements - spearheading security awareness and education - defining roles and responsibilities within the organizational structure -contingency planning, -instituting best practice standards.	-updating systems regularly -observing security matters strictly e.g. passwords issued secretly and not over the phone -test and maintain various system back ups -training the rest of the employees on the various IS security matters -advising management on various security software products to invest in -only allowing few selected well-trained employees to handle sensitive systems.	-observing all the relevant security measures mentioned in the organization's policy document -attending various training sessions organized by management -keeping their passwords secretively and changing them regularly -not opening and responding to emails from unknown sources -upgrading updates as soon as its required.

Source: Systems Administration on Network and Security Institute (2000); Abu-Musa (2010)

2.7 Research Conceptual Framework

Business rivals are heightening their sophistication, violating the defenses put in place in their targets' IS; in their wake, cyber attacks leaves immeasurable and insurmountable damage to the victim organization, (PwC, 2013). To keep up

with the adversaries' activities, organizations are forced to implement various cyber security measures.

This study proposes a conceptual framework for exploring the application of various cyber security measures and approaches in the wake of cyber security threats. The research will aim to answer the following key question: How do organizations react to the various cyber security threats that they are exposed to?

The GDT, as discussed under section 1.2, has been used to develop the conceptual framework of this research. For instance, the use of GDT countermeasures i.e. deterrence, prevention, detection and remedy has been seen to be dependent on the business environment in which an organization operates in and cyber security threats have been seen to drive the use of these GDT counter measures in businesses, (Schuessler, 2009). From this standpoint, the following key propositions have been formulated for testing in this research:

Proposition 1: The cyber security threats experienced are influenced by the business environment in which an organization operates in;

Proposition 2: The business reactions are influenced by the nature of threats to the business environment.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

According to Salifu (2008), ICT, especially the internet has greatly transformed formal and informal business transactions. However, ICT has become a double-edged sword providing endless opportunities to its users, but bringing with it a greatly increased information security risk and threats.

This study aims at establishing the manner in which businesses react to cyber security threats in the context of the Kenya business environment through the application of the GDT theory. This chapter specifically presents the methodology that was used to conduct the study. It covers the research design, the target population, sampling design, data collection instruments and procedures, the method of data analysis, research quality, and ethical considerations while conducting the research.

3.2 Research Design

The research design for this study was of a descriptive nature. Descriptive designs attempt to establish a relationship between factors, or variables. The study did employ descriptive research design so as to study the relationship of cyber security threats and business reactions. In describing the businesses reactions to cyber threats, a detailed review of various cyber security measures –an application of the GDT- was carried out. Descriptive research was appropriate in this study since it helped in the investigation of the ‘who, what, where, when or how much in an in-depth manner.

The research design was also of a correlation nature. Correlational research design is one in which the researcher gathers information and examines relations between variables, (Kabiru & Njenga, 2009). Correlation refers to the degree of relationship between two or more variables. This research aimed at establishing the degree of relationship between business reactions and cyber security threats. A positive correlation indicates that the two variables tend to change in the same direction

while a negative correlation indicates that the two tend to change in the opposite direction, (Nachmias & Nachmias, 2000).

All objectives were met through administering of questionnaires, (see appendix 5). The respondents were IT personnel and internal auditors of the various large organizations described as so by the Kenya Revenue Authority (KRA) criterion.

3.3 Population and Sampling

Kothari (1984); Engel, Holford and Helena (2010), define a population or universe as all the items under consideration in any field of inquiry. The population in this study constituted companies drawn from the same geo-location; this minimized on the effects of locational characteristics on the variables of interest. The companies selected were those described as large according to KRA definition. Large companies were selected as they were better placed to understand the cyber security risk and to implement the necessary controls to mitigate the risk. Large companies have been described by KRA as those companies which have a turnover of more than Ksh.750 million per annum. This definition was relied upon for this study as it offered ready data of the companies in Kenya that met this criterion.

The database had active 660 companies from 12 different sectors. In the formation of a sample, simple random sampling technique was used since it offered the participating elements an equal chance of being selected (Kothari, 2004; Mugenda & Mugenda, 1999). The sample size 'n' was formed by applying Slovin's formula as follows:

$$n = N / (1 + Ne^2)$$

Where:

n = Number of samples

N = Total population (660)

e = Error tolerance (0.05)

From the above formula, a sample size of 249 companies was selected. Profiling was then done so as to spread the number amongst the various sectors.

3.4 Data collection

Data was collected from both primary and secondary sources. Data from the primary sources was collected using the structured questionnaire. Information from this primary source was used to address all the objectives. Questionnaires were used since they are easily administered and they are faster. The close ended questions were for finding out the common aspects in the discussions whereas the open ended ones would have been useful in case of any personal views from respondents that would add value to the research. Five point likert scale was used to prepare the questionnaires. Secondary data mainly used survey reports, theories on the subject and previous researches on the subject. This data was collected by employing the technique of document reviews which narrowed on the various concepts under study. The data was specifically collected from internet sources i.e. relevant websites, newspaper articles, journals and text books. Information from these secondary sources was used to build the backbone of the study which further assisted in formulating the questionnaire.

3.5 Data Analysis and Presentation

Once data was collected, it needed to be analyzed and organized in a way that would ease understanding. Organization refers to the process of rearranging and reducing data so that it can be easily utilized, (Kabiru & Njenga, 2009). The main methods of organizing data are frequency tables, graphs and pie charts, (Cooper & Schindler, 2006). The information gathered in this research was organized in frequency tables and this was facilitated by use of statistical package for social scientists (SPSS V.16). The researcher then used the highest and lowest frequencies to interpret the collected data.

Graphs provide a visual representation of data. The main types of graphs include frequency histogram, frequency bar graphs, frequency polygons and line chart, (Kabiru & Njenga, 2009; Kothari, 2004). For this research, frequency bar graphs were used as enabled by SPSS, (V. 16). This enabled quick comparisons to be made between the data sets.

Collected data was further analyzed using SPSS (V.16) and Ms-Excel to obtain descriptive statistics. Some of the descriptive statistics that were computed included frequency mean and correlation coefficient. Correlation statistics determine the relationship between two variables. It gives the magnitude and direction of the relationship, (Kothari, 2004). Correlation coefficient was obtained for the following propositions:

Proposition 1: The cyber security threats experienced are influenced by the business environment in which an organization operates in;

Proposition 2: The business reactions are influenced by the nature of threats to the business environment.

Pearson's correlation was used at a 95% confidence interval to determine the correlation coefficient for the above propositions.

3.6: Reliability, Validity and Objectivity of the Research

The various elements of research quality include reliability, validity and objectivity as discussed below.

3.6.1: Reliability

An instrument or method is said to be reliable if it produces the same results whenever it is repeated and it is not sensitive to the researcher, the research conditions or the respondent, (Mugenda & Mugenda, 1999). The method adopted in this research was reliable as it was free of bias associated with the researcher, the subject or the research conditions. To measure the reliability of the data set, the split half method for estimating reliability was applied. Thus Cronbach's Alpha coefficient was calculated by use of SPSS (V.16) where a coefficient of 0.7 is deemed acceptable (Nachmias & Nachmias, 2000). For this data set, a coefficient of 0.847 was obtained thus the reliability test was passed.

Various tactics were further employed to establish reliability of the study, as recommended by Yin (1994). First, as many steps of the research as possible were documented. Furthermore, a formal and presentable database of documents was

prepared. This would enable other investigators to review the documents easily and make their own independent conclusions about the study.

3.6.2: Validity

Validity answers the question: do the instruments measure what they are supposed to measure? The instruments used in this study indeed measured what they were supposed to measure i.e. cyber security threats awareness and business' reactions.

Validity in this research was guaranteed through triangulation of data collection methods (questionnaire and secondary data). This is referred to as data triangulation; as the researcher collected information from multiple sources with an aim of corroborating the same phenomenon. By combining methods in the same study, researchers can partially overcome the deficiencies that flow from employing one method, (Yin, 1994; Nachmias & Nachmias, 2000).

3.6.3: Objectivity

Objectivity is the empiricist doctrine that the research process and design must be free of personal bias and prejudice (Mugenda & Mugenda, 1999). The research process adopted was free of all the personal values and views of the investigator. The results obtained were further analyzed as obtained without alterations that would have met the researcher's own personal biases and prejudice.

3.7 Ethical Issues

The researcher worked to ensure that respondents were protected and that minimum disruption was caused in their work. Therefore, there was informed consent i.e. willful participation and further the respondents were well informed about the aims of the study and any other relevant information.

The researcher provided a cover letter to the respondents to accompany the questionnaire that was used in the data gathering. This was important as firms might have been in competition and would have been keen to know who the researcher was and the manner which the information they offered would be used.

When constructing the questionnaire caution was taken not to use language or words that are biased against persons because of gender, sexual orientation, disability, age etc. The respondents were required to identify themselves only if they were comfortable to, as it was given as an optional question. Therefore anonymity was upheld to the upmost level. The results obtained were then summarized as they were originally without doctoring, suppressing, falsifying or inventing findings to meet either personal or specific people's needs.

CHAPTER FOUR

RESEARCH FINDINGS

4.1: Introduction

The study targeted a population of 660 corporations that were arrived at using the characteristics of the study as described in section 3.3 of this research. Using the Slovin's formula, a sample of 249 was selected. The amount was obtained as follows:

$$n = N / (1 + Ne^2)$$

where:

n=Number of samples

N = Total population (660)

e = Error tolerance (0.05)

thus:

$$n = \frac{660}{1 + (660 * (0.05)^2)}$$
$$=249$$

Out of 249 questionnaires distributed, 83 responses were obtained representing 33.33% response rate. Most of the responses obtained were from banking sector followed by service industry with percentage responses of 29% and 21.7% respectively. The relatively low response rate was as a result of the inherent weakness of using questionnaires as an instrument for data collection. This is especially so as the questionnaire could have been considered to be too lengthy and the information required could have been presumed to have been of a sensitive nature.

Descriptive statistics in form of frequencies, percentages, mean scores and cross tabulations were used to determine the pattern of data from various variables.

Pearson's correlation coefficient was used at a confidence level of 95% to detect associations and relationship of variables in the conceptual framework.

Respondent's satisfaction index was computed based on five point scale measurements; e.g. strongly agree, agree, neither agree nor disagree, disagree strongly or disagree. Mean score was computed in each measurement variable for all levels of satisfaction and agreement. This was converted into percentages and results were presented in frequency tables and graphs. Data was managed in Microsoft excel and analyzed using SPSS (V. 16).

4.2 General Information

The respondents were required to provide some general background information about their job descriptions, their length of stay in the organization and their specific industry affiliation. This information was significant as it did describe the targeted sample group and this would then facilitate the replication of this study.

4.2.1 Job Description of the Respondents

The survey presented the respondents with a multiple selection to indicate whether they were IT, internal auditors or other personnel. The specification helped the researcher narrow the respondents to the selected members of the organization who have the every-day mandate to protect their organizations against cyber security threats. Of the total responses received, 51 were IT personnel, 18 were internal auditors and 14 were others. The summary obtained is as shown in figure 4.1 below.

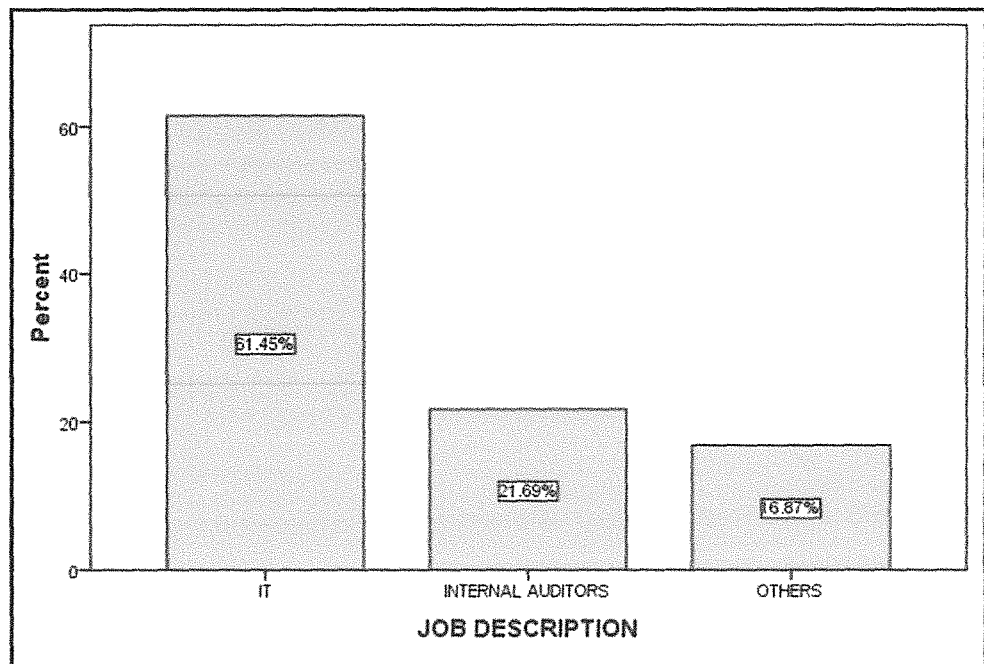


Figure 4.1: Bar Graph of Job Description

This shows that majority of the questionnaires (83%) were filled by the targeted personnel. The 'Others' group includes systems administrators, support engineers, system consultant, technician and system analyst. These too were well equipped to participate in the study as they had the technical knowledge required.

4.2.2 Duration of Service to an Organization

The survey presented the respondents with a single selection to indicate whether they were new or old employees. Duration of service to an organization would assist in establishing the respondents' degree of familiarity with their organizations' cyber security practices. Of the total responses obtained, 39 had worked for their organizations for less than 5 years, 33 for 5-10 years, 6 for 11-15 years, 3 for 16-20 years and 2 for more than 20 years, the findings are as shown in the figure 4.2 below.

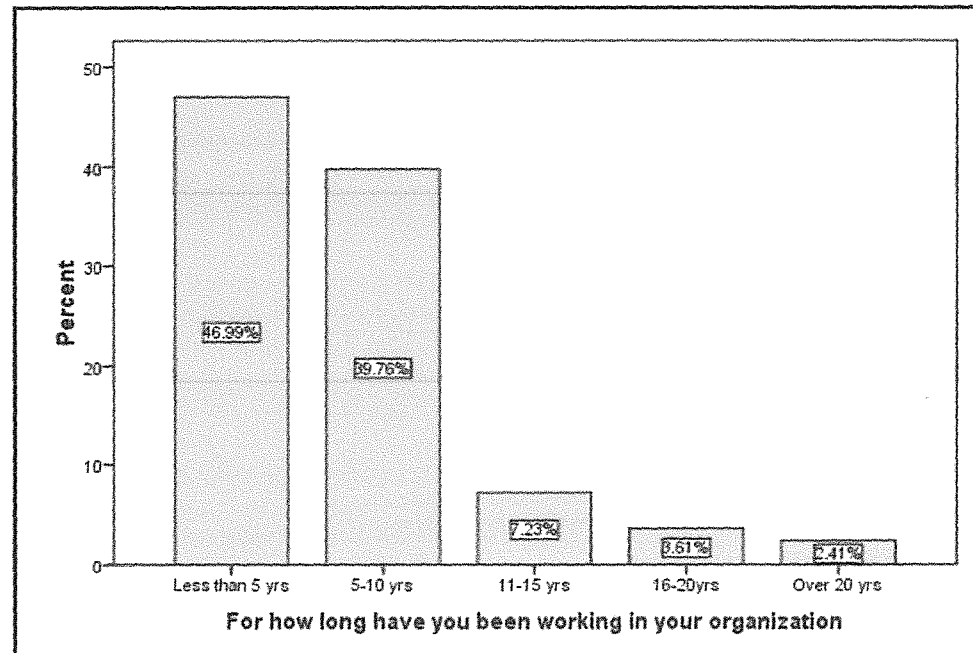


Figure 4.2: Bar Graph of Age of respondents

Majority of the respondents (47%) had worked for their organizations for less than 5 years. These were relatively well acquainted of the firms' operations and thus gave satisfactory responses. Less than 12% of the respondents had served their organizations for more than 10 years. This is in tandem with the nature of the profession of the target respondents. They shift jobs often in search for greater challenges and job satisfaction. (ITU, 2012).

4.2.3 Primary Function of the Organization

Of the total responses received, 19 were from banking and 1 from agriculture, oil& transport and construction and the rest of the results are as tabulated in Appendix 2.

4.3 Analysis of Cyber Security Threats' Characteristics

To answer the first objective as described in section 1.4 of the thesis, the respondents were asked on their perception of the various cyber security threats' characteristics. In reference to section 2.1, Cronin (2001); Smith and Rupp (2002);

Brenner (2004); Broadhurst (2006); Fletcher (2007); Etsebeth (2007); Salifu (2008); ITU (2011) discussed the various aspects that characterize cyber security threats.

4.3.1: Characteristics of Cyber Security Threats

The respondents were asked to gauge their degree of concurrence with the individual statements on a scale of 1-5. Where 1 stood for 'strongly disagree', 2 for 'disagree', 3 for 'neither agree nor disagree', 4 for 'agree' and 5 stood for 'strongly agree'. The responses are as shown in table 4.1 below.

Table 4.1: Characteristics of Cyber Security Threats

		Unobserve d ethical boundarie s	Identific ation of person responsi ble		Difficulty in prosecuti ng offenders	Low cost	Less reporting	Anonimity	
Valid	1	6.0	6.0	4.8	0	4.8	15.7	4.8	4.8
	2	4.8	4.8	20.5	8.4	2.4	18.1	9.6	4.8
	3	10.8	10.8	27.7	21.7	28.9	27.7	18.1	15.7
	4	25.3	25.3	27.7	42.2	34.9	21.7	32.5	34.9
	5	53.0	53.0	19.3	27.7	28.9	16.9	34.9	39.8
T ot al		100.0	100.0	100.0	100.0	100.0	100.0	100.0	

From the table 4.1 above, 53% strongly supported the statement that cyber security threats were borderless and had unobserved ethical boundaries. About 46%, 59%, 62% supported the following statements (respectively): that there is indeed difficulty in identifying persons responsible, that cyber security had multiple effects and there was difficulty in prosecuting offenders. This supported the literature as discussed by ITU (2011); Salifu (2008) in section 2.1. Less than 10% of the respondents were in disagreement with those characteristics except the low cost characteristic which had 15% respondents who disagreed with the statement that

cyber security threats require low costs to be actualized. This indicates that respondents do not perceive cyber security threats as requiring low costs to actualize them.

4.3.2 Rapid spread of Cyber Security threats

In a bid to investigate the cause of the rapid spread of cyber security threats in Kenya, (Kshetri, 2010), respondents were asked to rate the various characteristics' contribution towards the spread. Where the value of 1 stood for 'strongly disagree', 2 for 'disagree', 3 for 'neither agree nor disagree', 4 for 'agree' and 5 stood for 'strongly agree'. The results are as summarized in table 4.2 below:

Table 4.2: Table of Spread of Cyber Security Threats

	Borderless	Ethical boundaries	Identifying the responsible	Prosecuting offenders	Multiplier Effect	Low Cost	Few Reported Cases	Anonymity
Valid 1	53.0	31.3	2.4	3.6	3.6	10.8	3.6	1.2
2	25.3	30.1	8.4	7.2	3.6	16.9	15.7	6.0
3	10.8	27.7	13.3	15.7	19.3	30.1	16.9	10.8
4	4.8	7.2	48.2	38.6	41.0	30.1	48.2	43.4
5	6.0	3.6	27.7	34.9	32.5	12.0	15.7	38.6
Total	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0

As table 4.2 indicates, most respondents showed strong agreement with the statements implying that difficulty in establishing persons responsible, difficulty in prosecuting offenders, multiplier effect, low cost, few reported cases and anonymity contribute to the rapid spread of cyber security threats. However, only 6% and 3.6% respectively agreed that borderlessness and unobserved ethical boundaries contribute to the rapid spread of cyber security threats.

4.4 Awareness of Cyber Security Threats

To answer the second objective as described in section 1.4 of the thesis, the respondents were asked on their awareness levels of cyber security threats.

4.4.1 Awareness

When asked whether they had experienced cyber security threats in their organization, of the total responses received, 52 answered 'Yes', 21 answered 'No', 9 answered that they were not sure and 1 did not answer. This is as shown in figure 4.3 below.

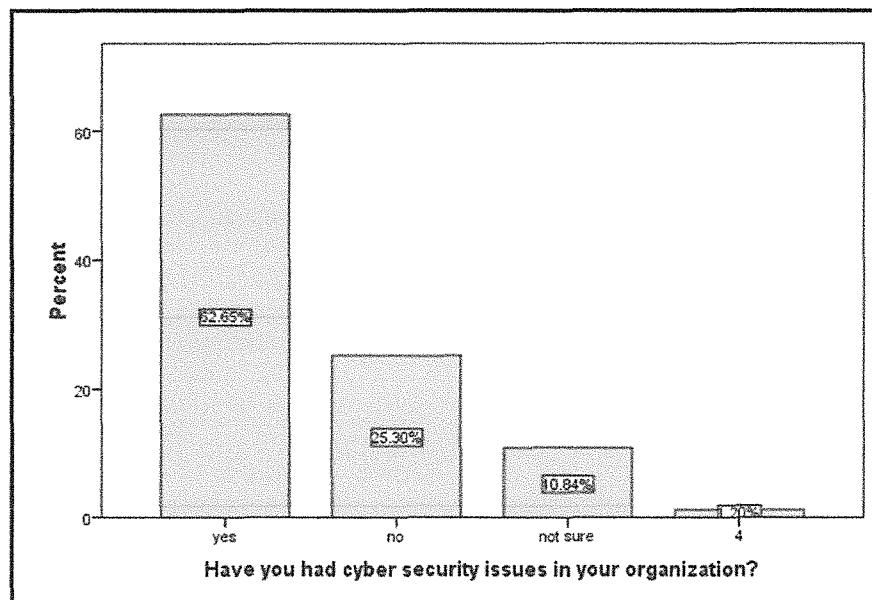


Figure 4.3: Bar Graph of individual Cyber security Threats awareness

Magutu et al. (2011) notes that cyber security threats are on the rise and a 63% 'Yes' response to this question is a confirmation of this. In addition, PwC (2011) survey shows that more organizations are reporting to having been victims of cyber fraud. This trend is likely to continue with the developments in the cyber world e.g. social networking and cloud computing etc.

4.4.2 IS Security Plan

When asked whether the respondents had IS Security plans in their organizations, 72 stated that they did have, 6 stated they did not have and 5 stated that they did not know. The results are as shown in figure 4.4 below:

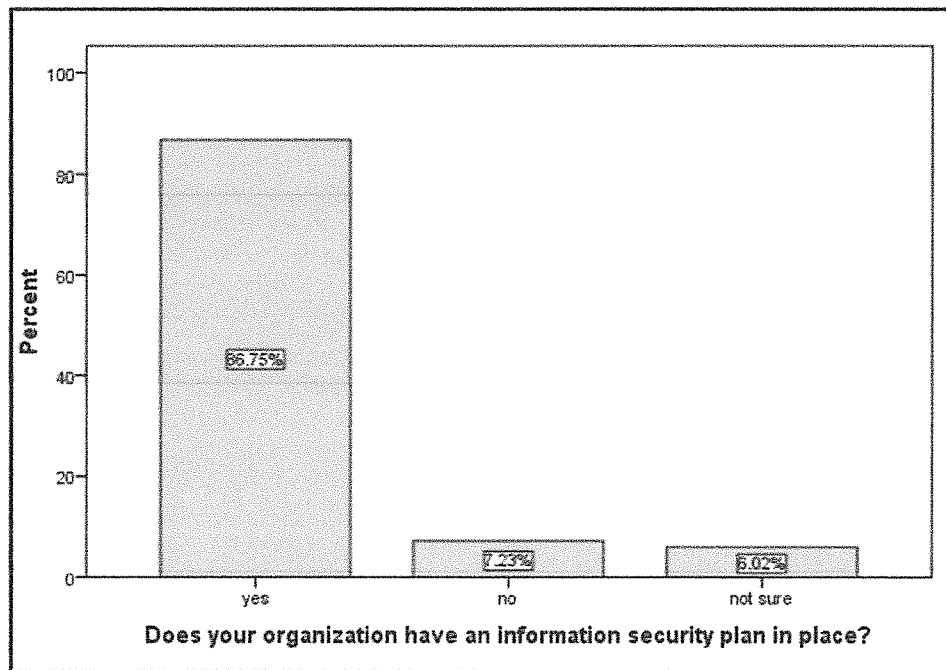


Figure 4.4 Bar graph of IS Security plan

A 67% positive response shows a step in the right direction as ITU, (2012) notes, presence of an IS security plan goes a long way in fighting the cyber security menace.

4.4.3 Budget Allocation

Fletcher (2007) suggests various technical and non-technical approaches could be considered for adoption by management in fighting cyber security threats. This requires the organization to allocate significant resources so as to put in place the various technical and non-technical countermeasures as stipulated in section 2.5.1.1 and 2.5.1.2 of the literature review.

According to Matt (2002); Trim (2005) a cost benefit analysis assists organizations to consider the various risks their assets are likely to face and the likelihood of their occurrence and compare this with the impact if they were to occur so as to establish the amount of investment they should put in securing those systems. In light of this, about 11% of the respondents stated that their organizations allocated less than 3% of their budgets to IT security, 13% of the respondents stated that their organizations allocated 4-7% of their budgets to IT security, 17% of the respondents stated that their organizations allocated 8-10% of their budgets to IT security, 22% of the respondents stated that their organizations allocated more than 10% of their budgets to IT security and the rest did not know the percentage. This is as shown in figure 4.5 below:

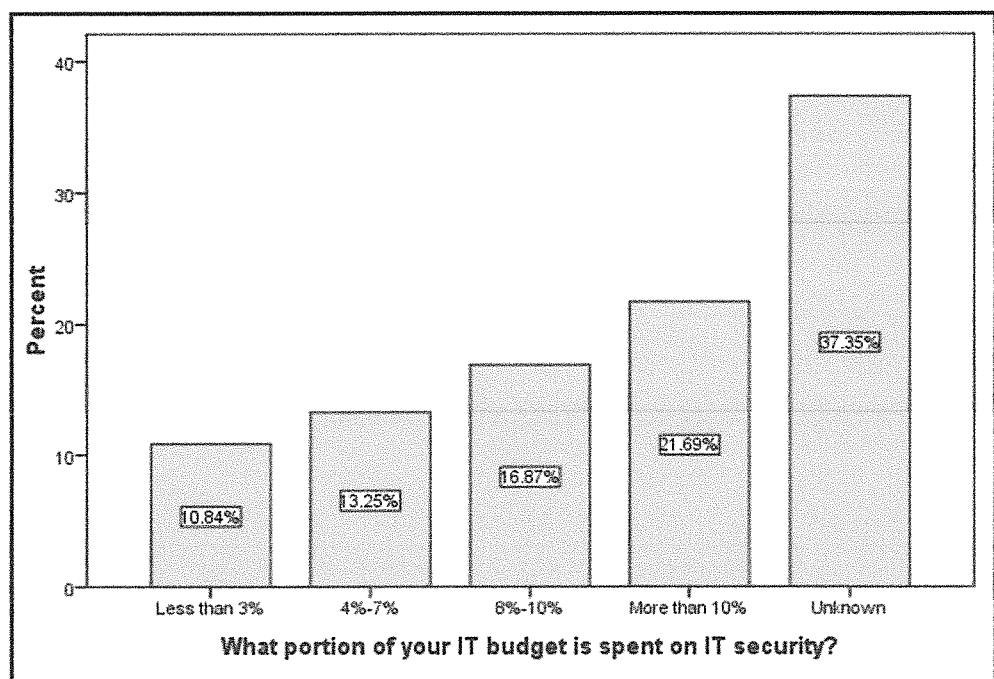


Figure 4.5: Bar graph of budgetary allocation

The variation in budget proportions spent on IT security is dependent on various factors e.g. nature of industry, organization's dependence on IT as discussed in section 2.2 of the literature review. A higher proportion would be desirable as it

would be an indication that the firms have put in place several counter measures thus gearing up for the cyber war.

4.4.4 Rating an organization's implementation of cyber-space security

The respondents were asked to rate their organization's implementation of cyber-space security. 42% stated that their organizations rated highly, 48% rated moderately and 10% rated lowly. The results are as shown in figure 4.6 below.

The various percentages are influenced by the factors laid out in section 2.2 of the literature review. High to moderate ratings may be an indication that the organizations rely on IT for 'Strategic benefits' as illustrated in the McFarlan's grid in section 2.2. Low rating may be an indication that the organizations rely on IT as 'Support mode' as discussed in section 2.2 of the McFarlan's grid.

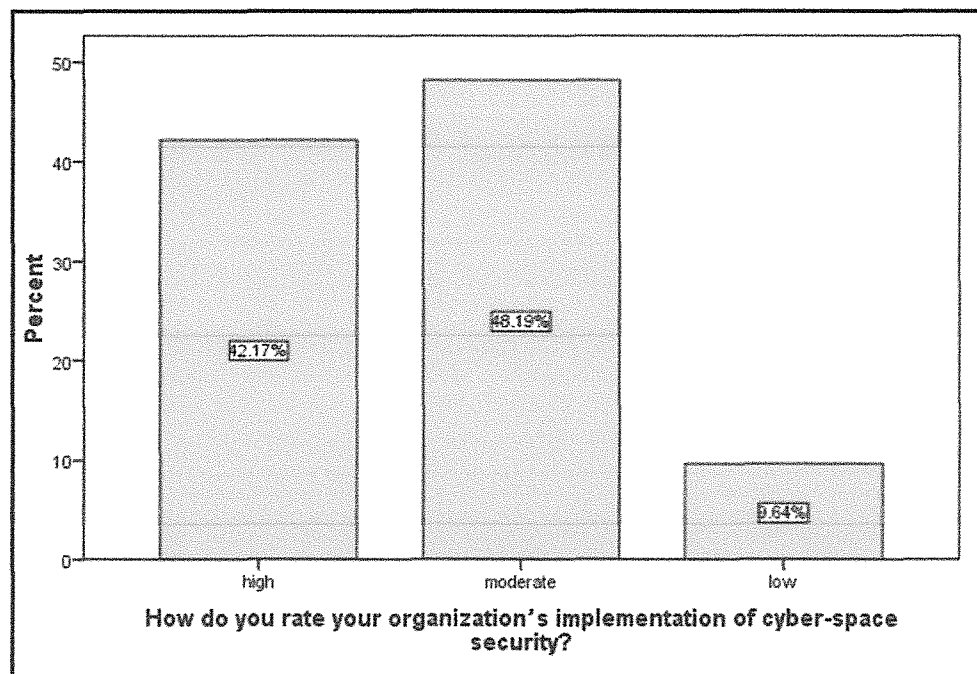


Figure 4.6: Bar graph of rate of Cyber-Space Security implementation.

The results are satisfactory as only less than 10% of the respondents rate their organization's implementation of cyber space security as being low. A higher

percentage is preferred as it shows firms have left fewer loopholes for exploitation by cyber criminals.

4.4.5 Cyber Space Security Strategies

Foryst (2010); NIST (2011) consider strategies as important in spelling out clear security agenda to the various stakeholders as it aids in communication. Respondents were asked whether they had cyber security strategies within their organizations. From the figure 4.7 below, 68.67% said that they had cyber security strategies in place, 13.25% said they had none and 18.07% said that they did not know.

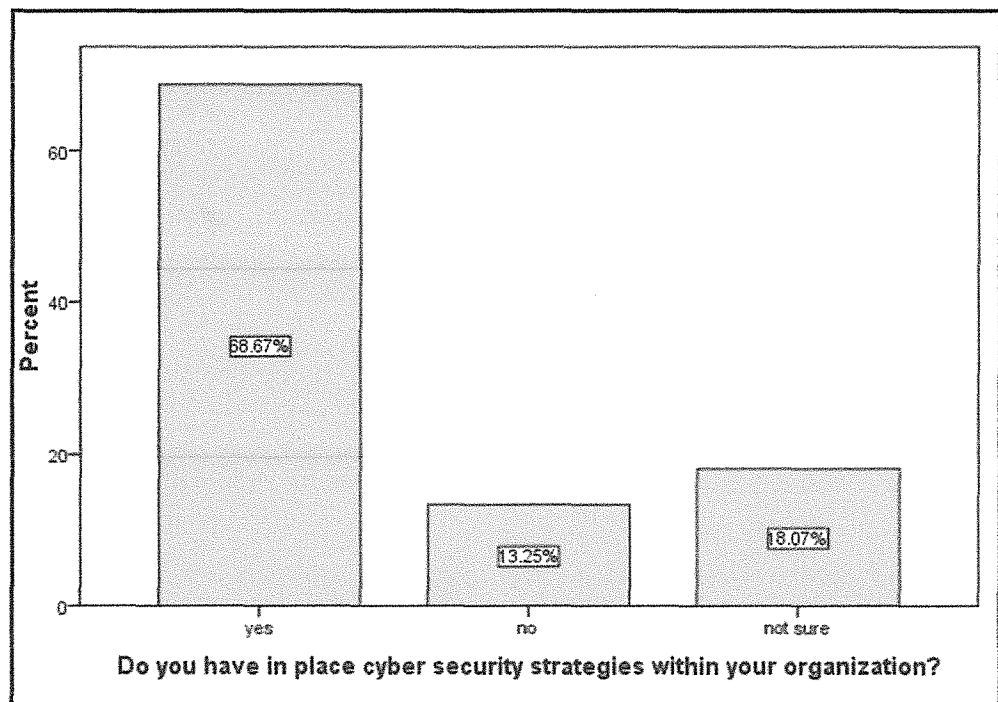


Figure 4.7: Bar graph of Presence of cyber security strategies within the organization

A significant number of respondents (69%) have cyber security strategies in their organizations. Such is a good trend that shows firms are recognizing cyber security as a key agenda that calls for due attention and strategic planning.

4.4.6 Cyber Security Strategies in Line with Environmental Requirements

Saini et al. (2012) note that the current cyber environment is faced by various unprecedented cyber security challenges. This could be due to various causes such as ubiquity of IT and wide adoption of e-commerce. Consequently, a need for an organization's cyber security strategies to be in line with the cyber security environment requirements arises. Respondents were asked whether they had cyber security strategies that were in line with environmental requirements. 48.19% answered 'Yes' to the question, 16.87% answered 'No' and 34.94% answered that they did not know. This is shown in the figure 4.8 below:

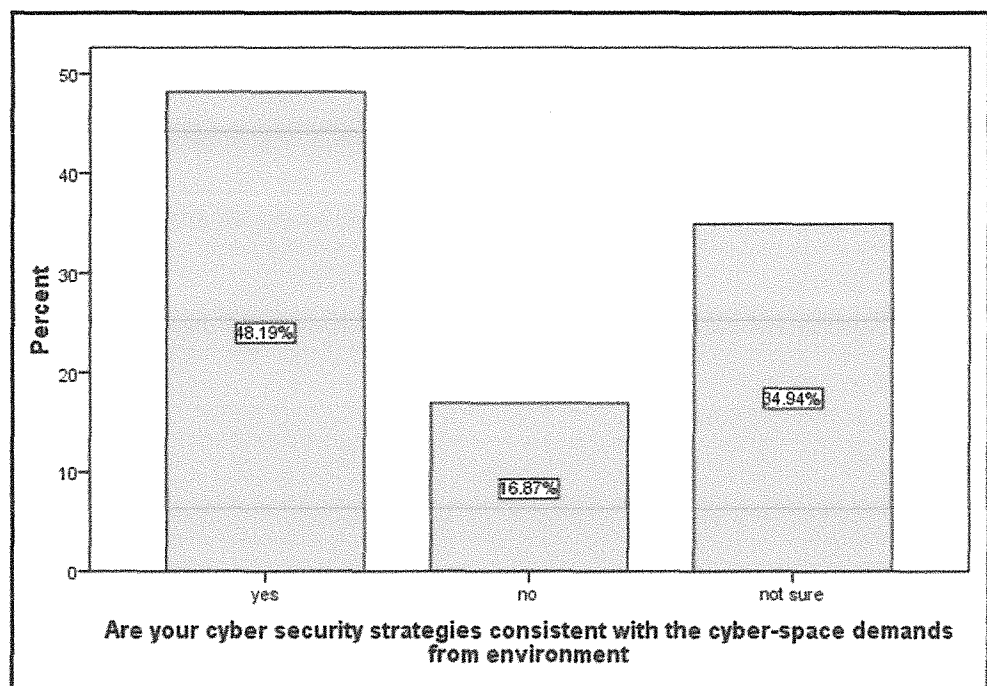


Figure 4.8: Bar Graph of individual Cyber security consistency with environmental Demands

Less than 50% of respondents claimed to have in place cyber security strategies that are consistent with cyber-space demand from environment. This is a low percentage

that needs to be improved so as to secure the business enough to enable it participate in e-transactions.

4.4.7 Cyber Security Strategies in Line with CCK Requirements

Guidelines stipulated by CCK aim at protecting the various stakeholders from cyber security threats. In reference to section 1.1.4.1, the CCK is in charge of regulating the communication networks in Kenya. Conformance with the guidelines and regulations will help users further secure their cyber environment, (PwC, 2011). Respondents were asked whether they had cyber security strategies that were in line with CCK requirements. From the responses received, 39.76% answered 'Yes', 7.23% answered 'No' and the other 53.01% responded that they did not know. This is as shown in the figure 4.9 below:

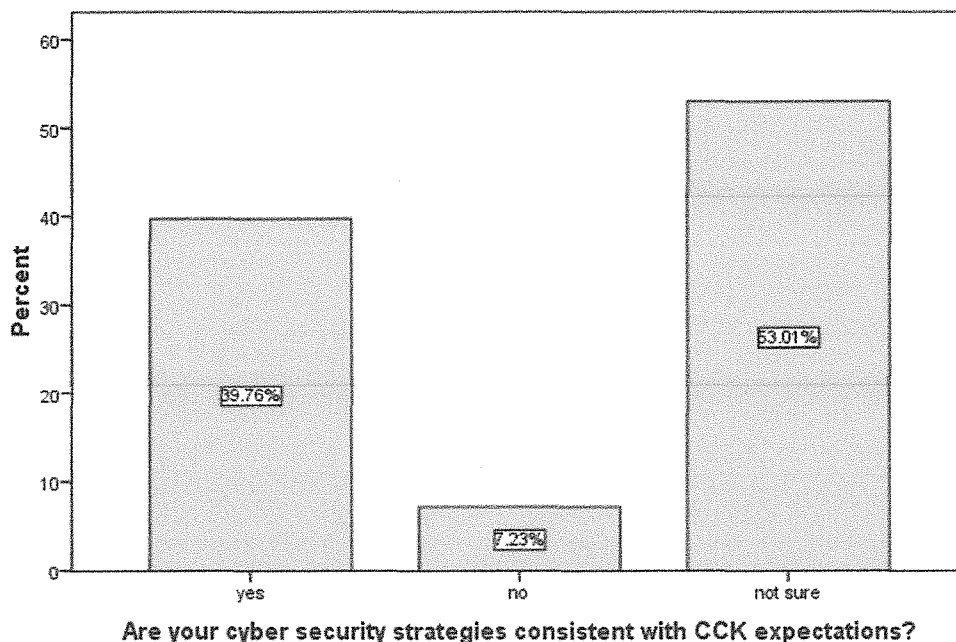


Figure 4.9: Bar Graph of individual Cyber security consistency with CCK Expectations

About 40% of respondents reported to have in place cyber security strategies that are consistent with CCK expectations. A higher conformance rate is recommended as this better secures the cyber environment in which the firms operate in.

4.4.8: The Cyber Security Primary Function

Cyber security primary function is dependent on the role IT plays in the various organizations as described in McFarlan's grid under section 2.2 of the literature review. The respondents were asked how they viewed their cyber security function. The results obtained are as shown on table 4.3 below:

Table 4.3: Cyber security primary function

	Frequency	Percent	Valid Percent	Cumulative Percent
An administrative job focused on granting user access and establishing degrees of privilege.	12	14.5	14.5	14.5
Critical to the long-term survival of the organization with emphasis on maintaining relationships with employees, business partners and government regulators.	24	28.9	28.9	43.4
Technically oriented with an emphasis on addressing authentication and authorization issues and maintaining physical security of computer resources.	30	36.1	36.1	79.5
As a resource to maintain compliance with information security standards and best practices.	17	20.5	20.5	100
Total	83	100.0	100.0	

From table 4.3 above, 36% of the respondents have their cyber security function as technically oriented with an emphasis on addressing authentication and authorization issues and maintaining physical security of computer resources. These fall on the 'Factory mode' of the McFarlan's grid. 43% of the respondents described their cyber security function as being critical to the long-term survival of the organization with emphasis on maintaining relationships with employees, business

partners and government regulators. These fall on the 'Strategic mode' of the McFarlan's grid. 15% of the respondents described their cyber security function as an administrative job focused on granting user access and establishing degrees of privilege. These fall on the 'Support mode' of the McFarlan's grid. 21% of the respondents described their cyber security function as a resource to maintain compliance with information security standards and best practices. These fall on the 'Turnaround mode' of the McFarlan's grid.

4.4.9: Composition of Information Security Team

McCrohan (2003) describes the various roles of the various stakeholders in the organization as regards positioning for the cyber war. The management's, IT employees' and the rest of the employees' roles are well stipulated in table 2.4 of the literature review. This shows that the cyber war is one to be taken seriously by all the relevant stakeholders and not one to be left in the hands of the IT staff only.

When asked the persons that mainly compose their IS security team, the following responses were obtained:

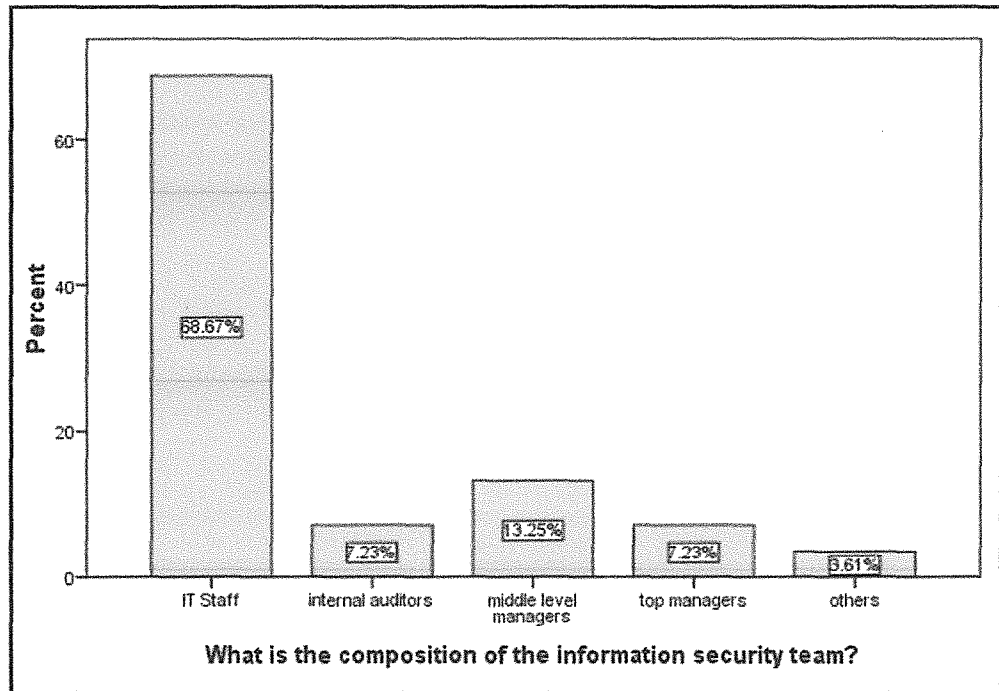


Figure 4.1.0: Bar graph of composition of information Security Team

The results show, 68.67% of respondents stated that IS security team was composed of the IT staff as was expected. However, only 13.25% and 7.23% stated that the IS security team was composed of middle level managers and top managers respectively.

4.5.0: Participation of Top Management in Information Security

Abu-Musa (2010) described the specific roles to be played by the management in combating the cyber security war. This is as shown in table 2.4 of the literature review. Respondents were asked the frequency of their top management participation in IS security planning. The results obtained are as shown in figure 4.1.1 below:

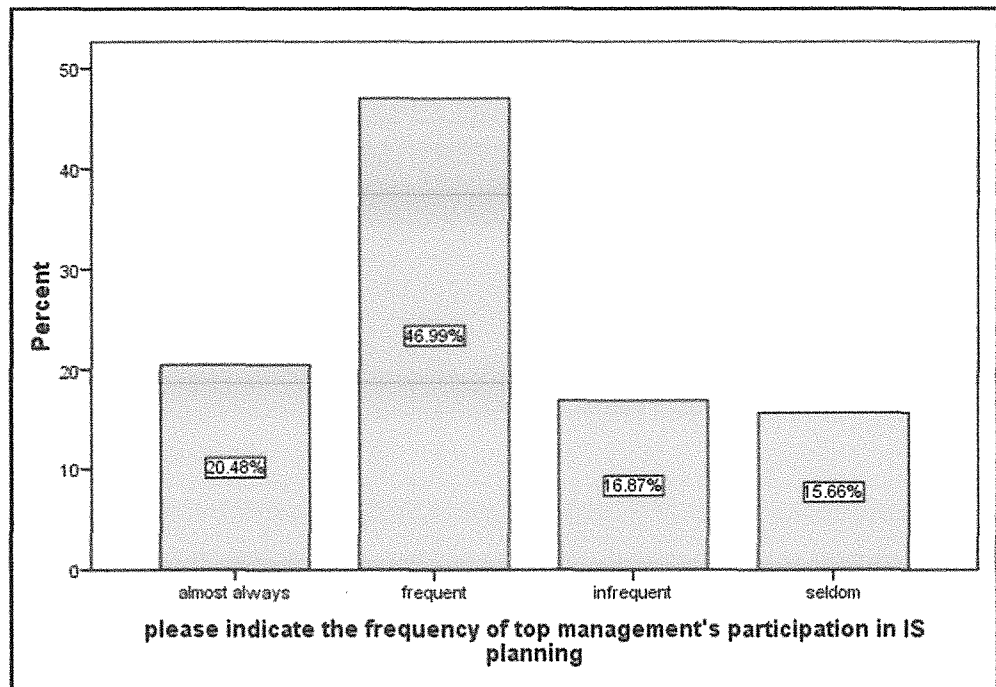


Figure 4.1.1: Bar Graph of Participation of Top Management in Information Security

Of the responses obtained, 46.99% stated that their top management was frequently involved in cyber security planning. This is a good trend that should be emulated by other organizations. Their frequent involvement is an indication that they have given the cyber security agenda top attention and this attitude will in effect spread to the rest of the employees.

4.5: Manifestation of Cyber Security Threats in a Business Environment

This section answered the third research question in section 1.5: How cyber threats manifest themselves in a business environment. In reference to section 2.4.2, the various ways through which cyber security threats manifest themselves include malware, phishing, identity theft etc.

4.5.1: Manifestation of Cyber Security Threats

Linking the cyber threats with the GDT theory discussed in section 2.7 of the thesis the following tables goes on to summarize the manifestation for the various cyber

security threats. Where 1 stood for 'strongly disagree', 2 stood for 'disagree', 3 stood for 'neither agree nor disagree', 4 stood for 'agree' and 5 stood for 'strongly agree'. The various cyber threats' manifestations are discussed below:

a) Malware:

As discussed in section 2.4.2 of the literature review, malware includes Trojan horse, viruses, computer worms and spyware. The table 4.4 below shows the respondents' view as regards malware deterrence, detection and prevention:

Table 4.4: Manifestation of malware

Statement	1	2	3	4	5	Total
a) Malware threat is easy to deter	2.4	8.4	18.1	34.9	36.1	100
b) Malware threat is easy to detect	6.0	20.5	36.1	21.7	15.7	100
c) Malware threat is easy to prevent	7.2	16.9	27.7	36.1	12.0	100

From the table 4.4 above, 36.1% of the respondents strongly agree that malware can be easily deterred. Another 21.7% strongly agree that malware is easily detected and 36.1% agree that malware are easy to prevent. Ease of deterrence, detection and prevention will reduce the chances of organizations falling victim of malware attacks.

b) Cyber Laundering:

The table 4.5 below shows the respondents' views as regards cyber laundering threat's ease of deterrence, detection and prevention:

Table 4.5: Manifestation of cyber laundering

Statement	1	2	3	4	5	Total

a) Cyber laundering is easy to deter	15.7	27.7	27.7	20.5	8.4	100
b) Cyber laundering is easy to detect	16.9	20.5	36.1	18.1	8.4	100
c) Cyber laundering is easy to prevent	24.7	39.1	12.0	17.2	6.9	100

From the table 4.5 above, about 43% of respondents disagree on the ease of deterrence of cyber laundering. Further on, only 8% and 6% of respondents agree on the ease of detection and prevention of this threat. This shows several firms have faced challenges in dealing with this threat. Much should be done to ensure that this threat is well managed as Saini et al. (2012) alerts organizations on the high prevalence of cyber laundering in the virtual environment.

c) Denial of service

Denial of service attacks aim at compromising the availability of systems files and networks to the authorized users, (ITU, 2011). The table 4.6 below shows the respondents' views as regards denial of service threat's deterrence, detection and prevention.

Table 4.6: Manifestation of Denial of service

Statement	1	2	3	4	5	Total
a) Denial of service is easy to deter	14.5	21.7	27.7	20.5	15.7	100
b) Denial of service is easy to detect	10.8	15.7	39.8	24.1	9.6	100
c) Denial of service is easy to prevent	15.5	23.7	21.7	21.5	17.7	100

From the table 4.6 above, respondents' views were split almost equally showing an about equal ratio of those agreeing to those disagreeing with the statements. A higher percentage on those who agree would be preferable as effects of a denial of service attack are very costly in terms of time, money and reputation to the victim if not promptly managed.

d) Phishing

Phishing, as discussed in section 2.4.2, is one of the various social engineering techniques that have been exploited in modern day. The table 4.7 below shows the respondents' views as regards phishing threat:

Table 4.7: Manifestation of phishing

Statement	1	2	3	4	5	Total
a) Phishing threat is easy to deter	17.2	26.5	30.1	18.9	7.2	100
b) Phishing threat is easy to detect	17.2	24.5	32.5	14.9	10.8	100
c) Phishing threat is easy to prevent	17.2	38.9	25.3	12.5	6.0	100

From the table 4.7 above, only about 7% strongly consider phishing as an easy threat to deter. Another 10% and 6% strongly agreed to the statements that phishing could be easily detected and prevented. More respondents were disagreeing than agreeing with the statements. Difficulty in the deterrence, prevention and detection should be tackled so as to alleviate the inherent weakness of the human person in the IT systems and hence beef up security.

e) Identity theft

Identity theft occurs where information is illegally obtained by cyber criminals in effect violating the confidentiality of the targeted systems, (Saini et al. 2012). The table 4.8 below shows the respondents' views as regards identity theft threat.

Table 4.8: Manifestation of identity theft

Statement	1	2	3	4	5	Total
a) Identity theft are easy to deter	20.8	24.1	28.9	17.7	8.4	100
b) Identity theft are easy to detect	19.6	22.9	25.3	18.9	13.3	100
c) Identity theft are easy to prevent	14.5	28.1	28.9	16.5	12.0	100

From the table 4.8 above about 28% were unsure on the ease of deterrence, detection and prevention of identity theft. About 44%, 41% and 43% of the respondents disagreed with the statements on the ease of deterring, preventing and detecting identity theft threat. The organizations should aim at dealing with the difficulty of deterring, preventing and detecting this threat as Sund, (2007) notes identity theft manifestation has shown much sophistication over the years.

f) System interference

As discussed in section 2.4.2, system interference threat is aimed at compromising the availability of system to the authorized users. The table 4.9 below shows the respondents' views as regards system interference threat:

Table 4.9: Manifestation of System interference

Statement	1	2	3	4	5	Total
a) System interference threats are easy to deter	20.8	15.7	32.5	13.7	17.2	100
b) System interference threats are easy to detect	27.2	24.5	23.7	11.3	13.3	100
c) System interference threats are easy to prevent	27.2	26.9	22.5	11.5	12.0	100

From the table 4.9 above, only 30%, 24% and 23% of the respondents admitted to the ease of deterring, preventing and detecting of system interference threat. This shows that the organizations are facing challenges in managing this threat.

4.5.2: Effects of Manifested Cyber Security Threats

This, as discussed in section 2.5 of the literature review, are the aftermath of the realization of cyber security threats. These could either be direct or indirect as shown in sections 2.5.1 and 2.5.2. The respondents were asked the effects of manifested cyber security threats where they were to show agreement or otherwise to the statements. Where 1 was for 'strongly disagree', 2 for 'disagree', 3 for 'neither agree nor disagree', 4 for 'agree' and 5 is for 'strongly agree'.

The findings are as shown in table 4.1.0 below.

Table 4.1.0: Effects of manifested threats

Effects of manifested cyber security threats	1	2	3	4	5	Total
Deletion of system files	3.3	6.9	22.9	34.1	32.8	100
Corruption of files and folders	9.3	8.1	14.5	28.1	40	100
Denied access to files	9.3	11.7	18.1	29.3	31.7	100
Forwarding of confidential information	6.9	4.5	13.3	23.3	52.2	100
Loss of customers	12.9	6.9	14.5	24.5	41.3	100
Loss of reputation	5.5	6.9	8.1	22.9	56.7	100
Loss of staff morale	15.7	16.9	15.7	22.9	28.9	100
Declined profitability	9.3	4.5	13.3	32.9	40.1	100
Loss of competitive advantage	10.8	15.7	10.8	18.1	44.6	100
Increase in legal costs	13.3	15.7	26.5	20.5	24.1	100
Loss of investors	14.5	14.5	8.4	21.7	41	100

From table 4.1.0 above, the top most rated effects of manifested cyber security threats include: loss of reputation (57%), forwarding of confidential information (52%) and loss of competitive advantage (44%). The above effects are not mutually exclusive and if they were to be felt simultaneously, their cumulative effect could drag a firm to its knees. This further emphasizes the need of having in place proper cyber security measures in place that deter, prevent and detect the various cyber security threats in the cyber space. The least rated effects include: loss of staff morale (15%), increase in legal costs (13%) and loss of investors (14.5%). This should not downplay their seriousness as the repercussions of their occurrence are of too of great magnitude to the firm.

4.6: Business Reactions to Cyber Security Threats

This answers the research question 4 as stipulated in section 1.5: How businesses have reacted to cyber security threats. The responses are classified in section 2.6 as being either technical or non-technical.

4.6.1: Technical approaches

Section 2.6.1.1 of the literature review described the various technical approaches to cyber security war; these acts as weapons that should help fight cyber criminals, (Salifu, 2008). The respondents were asked whether they had in place the various technological tools listed in table 4.1.1 below. The findings were as follows:

Table 4.1.1: Technical approaches

MEASURE	YES	NO	I DON'T KNOW
Anti-spam filter technology	81.9	9.6	6.0
Anti-piracy	56.6	22.9	19.3
Anti-jam	57.8	21.7	19.3
Anti-spoof	67.5	18.1	13.3
Anti-spyware	78.3	7.2	12.0
Honey-pot	47	22.9	27.7
Data back-up systems	89.2	4.8	3.6
Password	92.8	2.4	2.4
Anti-virus software	94	2.4	2.4
Encryption	84.3	9.6	3.6
User authentication	93.9	1.2	4.8
Digital signatures	66.3	19.3	12.0
Firewall	89.2	7.2	2.4
Patch	66.3	18.1	14.5

From the table 4.1.1 above, the most popular technical approaches- those that had a score above 80%- were anti-spam filter technology, data back-up systems, password, anti-virus software, encryption, user authentication and firewall. The least popular technical approaches- those that had a 'No' score above 20%- were anti-piracy, anti-jam and honey-pot. The popularity or otherwise of the above technical approaches is dependent on the severity of the threats they want to combat and the other factors are as discussed under section 2.2 in the literature review, for example, knowledge, cost and nature of sector etc.

4.6.2: Non-technical Measures

Benznosov and Beznosova (2007) note that non-technical measures will further help in solving cyber security issues as criminals have become increasingly aware of the social influence on the cyber war. The various non-technical measures are as discussed in section 2.6.1.2 of the literature review. The respondents were asked whether they had in place the various non-technical tools listed in table 4.1.2 below. The findings were as follows:

Table 4.1.2: Non-technical Measures

MEASURE	YES	NO	I DON'T KNOW
An operational cyber security policy document	75.9	15.7	7.2
You have instituted best practice standards	81.9	7.2	10.8
There is an existence of contingency plan	74.7	12	12
There is regular IT security training on the users	66.3	27.7	6.0
Audit of various system logs is carried out	86.7	8.4	4.8
Encourage security violation reporting	80.7	13.3	6.0
Has a management framework to initiate and control implementation of IS security	74.7	16.9	7.2
There is a plan for various contingencies	67.5	18.1	14.5
you work with external legal and regulatory entities to enforce and protect the organization's interests	69.9	20.5	9.6
Has scheduled, periodic reviews of the information systems security policy	78.3	12	9.6
Reinforces information security responsibilities to employees throughout their career	68.7	25.3	6.0
Has a formal reporting procedure for identified security incidents and weaknesses	71.1	14.5	14.5
Has a formal policy to protect against risks associated with obtaining files from unauthorized sources	80.7	10.8	8.4
Has established incident management procedures for information system security incidents	77.1	16.9	6.0

The most popular non-technical measures- with a rating above 80%- include: institution of best practice standards, systems audit, encourage security violation

reporting and existence of a formal policy. The most unpopular non-technical technical measures-with a 'No' rating above 20%- include: regular IT security training, working with external legal and regulatory entities, and reinforcement of information security responsibilities to employees. The organizations should work at improving the low ranked countermeasures for e.g. regular It training. Improvement in capacity development is necessary as a lack of knowledge on the side of employees would wash down the benefits of other measures that could have been in place. Moreover, poor IT security training or lack thereof would suggest that employees are potentially unaware of the risks that cybercrime presents to their organisation, (PwC, 2011).

4.7: Correlation findings

Pearson's correlation was used to test the following proposition of the conceptual framework in section 2.7 of the literature review.

Proposition 1: The cyber security threats experienced are influenced by the business environment in which an organization operates in

Correlations

Table 4.1.3: Cyber security threats versus industry affiliation

Correlations			
		industry affiliation	cybthreats
industry affiliation	Pearson Correlation	1	-.036
	Sig. (2-tailed)		.745
	N	83	82
Cybthreats	Pearson Correlation	-.036	1
	Sig. (2-tailed)	.745	
	N	82	82

The correlation coefficient is -0.036. This shows that a negative relationship exists between cyber security threats experienced and the business environment in which

an organization operates in. Only 0.036 of cyber security threats experienced are influenced by the business environment that one operates in. This shows that the various cyber attackers discussed in section 2.2.1 pay little regard to the business environment when launching their cyber attacks for as long as the target has the motivator that the attacker needs.

Proposition 2: The degree of business reaction is proportional to the severity of cyber security threats;

Table 4.1.4: Correlation Coefficient of Business reactions to cyber threats

		Correlations	
		Business Response	cybthreats
Business Response	Pearson Correlation	1	.671**
	Sig. (2-tailed)		.000
	N	82	82
cybthreats	Pearson Correlation	.671**	1
	Sig. (2-tailed)	.000	
	N	82	83

** . Correlation is significant at the 0.01 level (2-tailed).

A correlation coefficient measures the direction and strength of a relationship. A figure close to 1 shows that a strong relationship exists and a figure equal to 0 shows that the variables under consideration are not linearly related, (Kothari, 1984).

The correlation coefficient is +0.671. This shows a positive relationship between the measures adopted and the cyber threats in the business environment. The relationship is also relatively strong as it tends towards 1. This shows that 0.671 of business reactions is correlated to the nature of cyber security threats. The implication of this is that with increased severity of the threats to the business environment, the business reactions to be adopted will too be heightened.

Cyber security threats are thus good predictors of reaction in businesses. With the cyber security threats onslaught in the business environment that firms operate in, businesses will be forced to match up to the challenge as this will be their key to long term survival. Firms are already showing positive responses to this menace as a recent survey conducted by PwC indicated that a substantial number of respondents reported that their organizations exhibit the attributes of information security leaders, (PwC, 2013).

CHAPTER FIVE

DISCUSSION, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This chapter highlights the conclusions and recommendations based on the findings of this study. More specifically, the chapter discusses the summary of the objectives that guided the research, the methodology that was used to study those objectives and the findings resulting from the study. Further on the section linked the conclusions of the study to those that were earlier done and their contribution to the findings. Finally the section highlighted the implication, limitations and recommendations of the research.

5.2: Summary of Findings

This research has contributed to the conceptual and empirical understanding of the reaction of businesses to cyber security threats in the context of the Kenyan business environment. Based on the social identity theory, this research specifically aimed at establishing reaction of in-group members' to out-group members' activities. The study thus sought to analyze the various cyber security threats' characteristics, to determine the awareness levels of the in-group members in regard to the out-group members' tactics and the overall reaction of the business society to out-group members' activities, i.e. cyber security threats.

Descriptive and correlational research designs were applied and primary data was obtained by use of questionnaires. Questionnaires were circulated to 249 large organizations that operate within Nairobi County. Questions asked were mainly close ended and were of a five-point likert-type scale. Data obtained was analyzed by use of descriptive statistics and presented in frequency tables and bar graphs.

The findings from the 83 respondents show that cyber crime is a reality even in developing countries like Kenya and the following cyber security threats'

characteristics have contributed to the spread of the crime: borderlessness, unobserved ethical boundaries, anonymity, few reported cases, multiplier effect, difficulty in prosecuting offenders and difficulty in establishing persons responsible.

The study has further revealed that awareness level of the business community is relatively high. The respondents' awareness level is 62% and most reported to having in place IS Security plans in their organizations. Despite the relatively high awareness levels, the research revealed that barely 20% of the respondents' had adequate budgets allocated for fighting cyber security threats.

In this research, only 40% of respondents claimed to have implemented cyber space security in their organizations which were in line with environmental and CCK requirements. Majority of the respondents were not aware of the CCK cyber security requirements. This is an indication that CCK should dedicate more effort to sensitize the stakeholders on their guidelines as this would further improve compliance rates.

This research has further found out that firms rated malware, identity theft, system interference, malicious code and spam among their most frequently experienced threats (see Appendix 3). The least experienced threats include advance fee fraud, cyber squatting, copy right piracy, cyber espionage and cyber laundering.

Of the effects of manifested threats studied loss of reputation (56%), forwarding of confidential information (52%) and loss of competitive advantage (44%) were on the top of the list. The least rated effects include: loss of staff morale (15%), increase in legal costs (13%) and loss of investors (14.5%).

The most implemented technical approaches- those that had a score above 80%- were anti-spam filter technology, data back-up systems, password, anti-virus software, encryption, user authentication and firewall, (see table 4.1.1). The least rated include anti-piracy, anti-jam and honey-pot, (see table 4.1.1).

On top of the list of the non-technical measures implemented- with a rating above 80%- there were: institutions of best practice standards, systems audit, encouraged security violation reporting and existence of a formal policy. The most unpopular non-technical technical measures-with a 'No' rating above 20%- include: regular IT security training, working with external legal and regulatory entities, and reinforcement of information security responsibilities to employees, (see table 4.1.2).

From the propositions detailed in section 2.7, for the first proposition, only 3.6% of cyber security threats experienced were influenced by the business environment that a firm operates in. This shows that cyber criminals disregard the sector that a firm operates in and haphazardly attack any sector that attracts their attention.

For the second proposition, the analyses have further indicated that a business' reaction to cyber security threats has a positive relationship with the severity of the threats. A correlation coefficient of 0.626 explains that 62.6% of the variation in business reactions is related to the variation in the severity of cyber security threats. With further sophistication of the cyber security threats, businesses will heighten their security measures so as to gain an asymmetrical advantage over the cyber criminals.

5.3: Conclusion

The research revealed that cyber security threats are indeed characterized by borderlessness, unobserved ethical boundaries, anonymity, few reported cases, multiplier effect, difficulty in prosecuting offenders, low cost and difficulty in establishing persons responsible. This confirms the studies as conducted by Smith and Cronin (2001); Rupp (2002); Brenner (2004); Broadhurst (2006); Fletcher (2007); Etsebeth (2007); Salifu (2008); ITU (2011). The various stakeholders involved need to appreciate the uniqueness of cyber security threats-as compared to physical normal day threats-in setting up their cyber security strategies. For instance, the government should work on implementing the cyber laws strictly so as to prosecute more cyber criminals, (Ng'ang'a, 2009).

Most organizations showed high awareness and understood the significance of securing their systems. This agrees with the findings of survey conducted by Deloitte (2011) and contradicts the research findings of Kshetri (2010) which reported of low awareness levels in African countries. Awareness of the required security principles according to specific IS/IT circumstances is fundamental to security (Chang & Yeh, 2006). High awareness levels was supported by the claim of having in place IS strategic plans. The effectiveness of these IS security plans is yet to be established. An effective IS security strategic plan needs to stretch across the entire enterprise and work in tandem with many different functional areas (Ernst & Young, 2012). In the same vein, it is important that information security's goals are aligned not only with the overall enterprise-wide business goals, but also with the various departmental and functional goals (Deloitte, 2011).

Traditionally, firms have pigeonholed cyber security as an IT problem. The research findings confirm the same. But this is considered a risky approach that could leave firms open to attack, (PwC, 2011). A greater involvement by middle level and top managers would help in setting the right tone from the top of the organization to the bottom.

Few organizations reported to have in place adequate budgets for IS security implementation. This percentage is bound to improve with further awareness and sensitization of the stakeholders. As organizations around the world are seeing the rise in the threat levels, some are responding by spending more and adjusting their priorities, (Ernst & Young, 2012). Moreover, due to the influx of newspaper articles outlining security breaches, increased regulation and corporate governance pressures, more money and attention is being spent to win back consumer trust, (Deloitte, 2004). Therefore, in Kenya businesses too, a more significant budget allocation is anticipated in the near future.

This research showed that achieving compliance with regulations had been an important driver of information security for only about 50% of the respondents. This is in conformance with the study conducted by Tsohou, Kokolakis, Lambrinoudakis

and Gritzalis (2010), PwC (2011), Ernst and Young (2012) which indicated that stronger adherence to regulatory requirements had significantly determined how organizations manage information security risk. The compliance level is relatively high though it could also be an indication that CCK regulators have not put in place punitive clauses for the non-compliant persons or that regulators have been insufficient in dealing with cyber crime, (Kshteri, 2010).

This research has further found out that firms rated malware, identity theft, system interference, malicious code and spam among their top five most frequently experienced threats. This confirms previous studies conducted by Magutu, Ondimu and Ipu (2011). Consequently, these are also the areas where most businesses have protection in place – over 80%- for their networks, (see table 4.1.1). Conversely, businesses undermine these protections by failing to educate their employee not to open dubious e-mail attachments, not to respond to emails from suspicious sources and thus waters down their earlier investments in the various technological tools. This is an emphasis on the need for training of staff and other stakeholders alike.

The direct effects of cyber security threats compromise the confidentiality, availability or integrity of systems and data files. When either of the three is violated then further indirect losses e.g. loss of competitive advantage, loss of reputation is experienced. As with the survey conducted by Ernst and Young, (2008) more respondents in this research seemed to rate loss of reputation higher than loss of revenue as an effect of the realization of a cyber security threat. Paul van Kessel, Global Leader of Ernst & Young's Technology and Security Risk Services, commented:

“A good brand and reputation can take years to build but can be severely damaged or even destroyed by a single security incident. Now, the desire to protect brand and reputation is motivating many organizations to do more than just tick regulatory and corporate compliance boxes.” (Ernst & Young, 2008; pg 32).

Most respondents had engaged the use of various technical tools to counter the cyber security menace. In contrast, a recent survey conducted by PwC reported of a counterintuitive trend where there was a decreased deployment of many basic information security tools, (PwC, 2013) e.g. malicious code detection tools. This should be corrected as the various IS security tools, go a long way in detecting and preventing cyber security threats occurrences.

Training of employees was seen to be low across the sectors. This is consistent with the research findings of Deloitte, (2004), Magutu et al. (2011), and PwC (2013). The training of employees should be improved as it would go a long way to ensure the whole firm is well equipped towards fighting a common enemy, (ITU, 2012).

Firms across the sectors differ in the deployment of security products to address the cyber concern. Businesses and consumers in leading e-commerce sectors are more likely to be cyber-crime targets compared with other less e-commerce-ready industries, (Kshteri, 2010). As Appendix 4 shows, the e-commerce sectors i.e. banking and services sectors were seen to rank highest in their implementation of cyber security counter measures. More is yet to be done by the leading e-commerce sectors as the recent statistics show that Kenyan banks suffer losses amounting to Ksh. 2.1 billion each year, (Ng'etich, 2012).

A major component of cyber security is a nation's ability to deter, detect, investigate and prosecute cyber criminal activities. Weaknesses in any of these areas can compromise security not only in that country but also around the globe (Salifu, 2008). Globally, years of investment have been reported to pay off as Asia leads the world in security practices and performance, (PwC, 2013). Kenya too can be a leader in applying best in class cyber security practices and approaches if they adopt the various suggestions extended from this research.

5.4: Research implications

As deduced from the general deterrence theory, stakeholders should consider adopting deterrent, preventive, detective and usage of remedies to influence cyber security rates. Deterrent and preventive measures are seen to work before the threats

are actualized. Detective measures and usage of remedies are seen to be at work after the occurrence of the attack. Stakeholders should deliberately attempt to implement proactive vulnerability management -rather than reactive- to prevent security breaches from occurring (Deloitte, 2011; Magutu et al., 2011).

A recommended proactive approach is the sensitization and training of the public on the various cyber security threats that exist, the forms in which they can manifest and the ways to prevent and detect the threats. Ernst and Young (2004) reckoned that inadvertent mistakes by employees or external parties were the most significant source of financial loss. This loss could be mitigated by training and education. The organization usually has various stakeholders: the customers, employees, suppliers, shareholders etc. all these should be sensitized on the cyber security agenda as security lapse on one end would ultimately affect the entire organization.

The research statistics showed that the most senior people in organizations are not placing enough emphasis on the importance of managing the cybercrime threat. The CEOs and the boards of the firms should be involved as they will offer leadership that instils a cyber risk-aware culture across the organization, (PwC, 2011).

Social media sites like Facebook, Twitter and LinkedIn might not be the real source of cybercrime, but criminals can use them to social engineer cybercrime more effectively (e.g. vishing attacks). For example, they can use them to collect information on a target or install malware on the target's computer, all very easily, (PwC, 2011; Kshteri, 2010). Kenya government has recently reported to be having trouble in dealing with social media traffic, (Kamunyu, 2013). The government should implore the help of trained persons to pin down the fraudsters who are hiding behind the social media sites.

Organizations should consider setting up a cyber incident response team that can act and adapt quickly- the organization can then track, risk- assess and deal with an incident as soon as it is spotted anywhere in the business, (PwC, 2011).

There is need for increased collaborations between the public and private sectors, (Korsell & Krister, 2001). This partnership will help in bringing down the social stigma (amongst in-group members) of being a victim of out-group members' activities. Ideally, businesses would come together out of their own volition to share experiences and establish common frameworks and solutions. It has worked for other issues and it may be the best choice too as organizations may be forced to stem the flow of impending regulation, (Ernst & Young, 2012).

Active participation by Kenya in international collaborations would be an extension of the above. Various organized structures and institutions that are at the fore front of combating cybercrime namely: the various economic blocs for e.g. East African Community, (EAC), United Nations, (UN) and international police, (INTERPOL) - have the mandate of uniting countries across the globe and further share ideas on how to fight the common enemy, (Akuta et al. 2011). Kenya would benefit from these collaborations as she will get to learn from others' experiences, challenges and forge the best way forward.

Quite a number of security standards are incessantly being released; a few of them offer guidelines, others endorse best practices, while others have been used as a basis for certification e.g. ISO/IEC 27001:2010, (Tsohou, 2010). Kenya has been seen to adopt ISO standards which offer guidelines and are too used as a basis for certification. Kenyan legislators should go a step further to educate various stakeholders of the benefits of adopting and conforming to these best practices.

Kenya government through the Ministry of Information and Communication should see to it that the NPKI project initiated goes to its completion so that anonymity in the virtual world gets to be monitored through the issuance of digital signitures, (Mumo, 2013).

Kenya also lacks the legal framework that would enable it achieve its objectives under the ICT pillar of vision 2030, (Ng'ang'a, 2009; Ksheteri, 2010). Amendments to the current legislation are recommended as to boost the cyber security initiative that would aid the realization of the ICT pillar of vision 2030, (Mumo, 2013).

5.5: Limitations of the Study

The study was challenged by the inherent weaknesses of questionnaires for e.g. use of close ended questions left little or no scope for respondents to qualify the meaning of their answers. Further on the researcher was not in a position to know whether the intended persons indeed filled the questionnaire.

The findings pertain exclusively to the IT personnel's and internal auditor's view point. The viewpoint of management and the rest of the employees would be at variance with the findings that were obtained from this research.

The low response rate limit the ability to generalize the information gathered as the sample may be unrepresentative of the target population. Generalization was further inhibited as the study was limited to large organizations. Small and medium sized enterprises may have revealed a different trend altogether.

5.6: Recommendations for Further Research

Areas of further research that were identified include:

The study was limited to large organizations in Nairobi metropolitan region. It did not consider small and medium sized enterprises in other counties. It would be interesting to ascertain their awareness levels to cyber security threats and hence their reactions to the same. This would highlight the differences, if any, and conclusively describe the reactions of businesses to cyber security threats in Kenya.

Most businesses had in place various deterrent, detective and preventive measures as stipulated by the GDT theory yet they reported to have suffered from various cyber attacks. A similar study could be carried out to establish why cyber security threats still persist amidst the various GDT measures that have been implemented in businesses.

Further research, too, should be carried out in the same area with the application of other data collection methods e.g. interviews and other data analysis techniques e.g. cross-tabulations. Other business stakeholders-both internal and external- could be interviewed too to get alternative viewpoints as regards this subject matter.

REFERENCES

- Abu-Musa, A. (2010). Information Security Governance in Saudi Organizations: an Empirical Study. *Information Management & Computer Security*, 18(4), 226 – 276.
- ACCA (2009). *Business Analysis*. Kaplan publishing.
- Adomi, E.E. & Igun, S.E. (2008). Combating Cyber-crime in Nigeria. *The Electronic Library*, 26 (5), 716-25.
- Ajala, E.B. (2007). Cybercafes, Cybercrime Detection and Prevention, *Library Hi Tech News*, 24 (7), 26 - 29 .
- Akuta, E. A., Ong'oa, I. M., Jones, C.R. (2011) : Combating Cyber Crime in Sub-Sahara Africa; A Discourse on Law, Policy and Practice. *Journal of Peace, Gender and Development Studies*, 1(4), 129-137.
- Amoroso, E. (1994). *Fundamentals of Computer Security Technolog*. Prentice Hall.
- Ampratwum, E.F.(2009). Advance Fee Fraud "419" and Investor Confidence in the Economies of Sub-Saharan African (SSA). *Journal of Financial Crime*, 16 (1), 67– 79.
- Anita, D. (2000). *What Does Computer Security Breach Really Cost?* Secure Decisions.
- Atkinson, S., Johnson, C. & Phippen, A. (2007). Improving Protection Mechanisms by Understanding Online Risk. *Information Management & Computer Security*, 15 (5), 382 – 393.
- Beznosov, K. & Beznosova, O. (2007). On the Imbalance of the Security Problem, Space and its Expected Consequences. *Information Management & Computer Security*, 15 (5), 420 – 431.
- Bhattacharya, D. (2011). Leadership Styles and Information Security in Small Businesses. *Information Management & Computer Security*, 19 (5), 300-312.
- Bishop, M. (2002). *Computer Security, Art and Science*. Pearson Education .
- Brenner, S. (2004). Cybercrime Metrics: Old Wine, New Bottles. *Virginia Journal of Law and Technology*, 9 (13), 1-53.

- Broadhurst, R. (2006). Developments in the Global Law Enforcement of Cybercrime. *Policing: An International Journal of Police Strategies & Management*, 29(3), 408-33.
- Bronk, C., Monk, C., & Villasenor, J. (2012). The Dark Side of Cyber, Finance. *Survival: Global Politics and Strategy*, 54 (2), 129-142.
- CBK (2013). *Value of Virtual Payment Transactions*. Retrieved March, 6, 2013, from <http://www.cbk.go.ke.html>
- CCK (2013). *CCK 2012/2013 Reports*. Retrieved February, 8, 2013, from <http://www.cck.go.ke.html>.
- Champlain, J.J. (2003). *Auditing Information Systems* (2nd Ed.). John, Wiley & Sons Inc.
- Chang, S.E. & Ho, C.B. (2006). Organizational Factors to the Implementing Information Security Management. *Industrial Management & Data Systems Effectiveness*, 106 (3) 345 – 361.
- Chang, A.J. & Yeh, Q.J. (2006). On Security Preparations Against Possible IS Threats Across Industries. *Information Management & Computer Security*, 14 (4), 343 – 360.
- Cheswick, W.R., Bellovin, S.M. & Rubin, A.D. (2003). *Firewalls and Internet Security* (2nd Ed.). Pearson Hall.
- CISA (2012). *Certified Information Systems Auditor Review Manual-2012*, ISACA.
- CISCO (2005). *Network, Security Fundamentals*. CISCO Press.
- CMA (2012). CMA Management Supervision Control Report 2012. Retrieved May, 23, 2012, from <http://www.cmamangement-supervision-internal-control-report2012.com>
- Cole, K., Chetty, M., Larosa, C., Rietta, F., Schmitt, D.K., & Goodman, E. (2008). *Cyber Security in Africa: An Assessment*. Georgia Institute of Technology
- Cronin, B. (2001). Information Warfare: Peering Inside Pandora's Postmodern Box. *Library Review*, 50 (6), 279 – 295.
- Deloitte (2004). *Global Security Survey 2004*, Author.
- Deloitte (2011). *East Africa Application Security Survey 2011; Safeguarding the Future*, Author.

- Dion, M. (2011). Corruption, Fraud and Cybercrime as Dehumanizing Phenomena. *International Journal of Social Economics*, 38(5), 466 – 476.
- Donato, L. (2009). An Introduction to How Criminal Profiling Could Be Used as a Support for Computer Hacking Investigations. *Journal of Digital Forensic Practice* 2(4), 183- 195.
- D'Ovidio, R. (2007). Technology issues. *Security Journal* 20, 45 – 49.
- EEL, (2010). *Principles for Cyber Security and Critical Infrastructure Protection*. Retrieved on July 27, 2012, from <http://www.eei.com>
- Eeten, M. J. & Bauer, J.M. (2008). Economics of Malware: Security Decisions, Incentives and Externalities. *OECD Science, Technology and Industry Working Papers*, 2008/01, OECD Publishing. Retrieved from <http://dx.doi.org/10.1787/241440230621>
- Engel, L.C., Holford, J. & Helena, P.W. (2010). Effectiveness, Inequality and Ethos in Three English Schools. *International Journal of Sociology and Social Policy*, 30 (3), 140 – 154.
- Ernst & Young (2008). *Global Information Security Survey 2008*. Author.
- Ernst & Young (2012). *Global Information Security Survey 2012- Fighting to Close the Gap*. Author.
- Etsebeth, V. (2007). Malware: The New Legal Risk. *The Electronic Library*, 25 (5), 534 – 542.
- Fletcher, N. (2007). Challenges For Regulating Financial Fraud in Cyberspace. *Journal of Financial Crime*, 14(2), 190-207.
- Foryst, C.A. (2010). Rethinking National Security Strategy Priorities, *International Journal of Intelligence and Counter Intelligence*, 23(3), 399-425.
- Gordon, L.A., Gordon, M.P.L. & Sohail, T. (2003). A Framework For Using Insurance for Cyber Risk Management. *Communications of the ACM*, 4 (3), 81-5.
- Grabosky, P. & Smith, R. (2001). *Telecommunication Fraud in the Digital Age: The Convergence of Technologies-Crime and the Internet*. Routledge, London.
- Halsall, F. (2005). *Computer Networking and the Internet* (5th Ed.). Pearson Education.

- Hall, J.H., Sarkani, S. & Mazzuchi, T.A. (2011). Impacts of Organizational Capabilities in Information Security. *Information Management & Computer Security*, 19 (3), 155 – 176.
- Harrington, J.L. (2005). *Network Security*. Morgan Kaufmann Publishers.
- Hong, K. S., Ching, P.H., Chao, L. R. & Tang, J.H. (2003). An Integrated Systems Theory of Information Security Management,” *Information Management & Computer Security*. 11(5), 243-248.
- ITU, (2011). *Understanding Cybercrime: A Guide for Developing Countries*. Retrieved on June 19, 2012, from <http://itu.int/thephenomenonofcybercrime/>
- ITU, (2012). *Cyber Security Legislation*. Retrieved on August 12, 2012, from <http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html>
- Jenkins, J. (2001). *Organizational IT Security Theory and Practice: And Never the Twain Shall Meet?* SANS Institute.
- Jones, B.R. (2007). Cyber Criminals and Society, *The Journal of Criminal Law and Criminology*, 9 (2), 601-629.
- Kabiru, M. & Njenga, A. (2009). *Research, Monitoring and Evaluation*, Focus Publishers.
- Kamunyu K. (2013, March). Hate Speech as a Tough Nut for the Government. *Daily Nation*, p. 4.
- KBE, (2005). *Kenya Business Environment Report*. Retrieved on June 2012 from <http://www.kenyabusinessenvironmentreport2005.com>
- KCA, (2008). *The Kenya Communications (Amendment) Bill of 2008*. Retrieved on June, 8, 2012, from <http://www.kenyacomunicationsamendmentbill2008/>
- Keene, S. D. (2011). Emerging Threats: Financial Crime in the Virtual World. *Journal of Money Laundering Control*, 15 (1), 25 – 37.
- Korsell, E.L. & Krister, S. (2001). IT-Related Crime – Old Crimes in a New Guise, But New Directions Too. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, 2(1), 5-14
- Kothari, C. R. (1984). *Quantitative Techniques* (3rd Ed.). Vikas Publishing House.
- Kshetri, N. (2010). Diffusion and Effects of Cyber-Crime in Developing Economies, *Third World Quarterly*, 31, (7), 1057–1079.

- Lee, J. & Lee, Y. (2002). A Holistic Model of Computer Abuse Within Organizations. *Information Management & Computer Security*, 10 (2), 57-63.
- Li, X. (2006). Cyber Security as a Relative Concept. *An International Journal*, 18, 200-6.
- Magutu, P.O., Ondimu, G.M. & Ipu, C.J. (2011). Effects of Cybercrime on State Security: Types, Impact and Mitigations with the Fiber Deployment in Kenya. *Journal of Information Assurance & Cybersecurity*, 12 (9), 3-16.
- McConnel, (2000). *Cybercrime and Punishment, Archaic Laws Threaten Global*. Information McConnel International LLC.
- McCrohan, K.F. (2003). Facing the Threats to Electronic Commerce. *Journal of Business & Industrial Marketing*, 18 (2), 133 – 145.
- Mell, P., Bergeron, T. & Henning, D. (2005). Creating a Patch and Vulnerability Management Program. *National Institute of Standards and Technology Special Publication*, 2 (2), 800-40.
- Microsoft, (2012). *Computer Security*. Retrieved on August 3, 2012, from <http://www.microsoft.com/security/pc-security/firewalls-what-is.aspx>
- Montesino, R., Fenz, S. & Baluja, W. (2012). SIEM-based Framework for Security Controls Automation. *Information Management & Computer Security*, 2(4), 6- 19.
- Mugenda, O. & Mugenda, A.G. (1999). *Research Methods: Quantitative and Qualitative Approaches*. African Centre for Technology Studies.
- Mumo M. (2013, April). Online System to Make Virtual Trading Safer. *Daily Nation*, p.8.
- Nachmias D. & Nachmias, C.F. (2000). *Research Methods in the Social Sciences* (5th Ed.). Arnold.
- Ng'ang'a, A. M. (2009). Toward a Regional ICT Hub: Need for Cyber Laws in Kenya. *Information Security Journal: A Global Perspective*, 18(1), 47-50
- Ng'etich P. (2012, April). Kenya Loses Ksh.3 Billion to Cyber Crime Every Year. *Daily Nation*, p.23.
- NIST (2011). *Glossary of Key Information Security Terms*. US Department of Commerce.

- Njihia M. (2012, July). Securing the Kenya Cyber Space. *Business Daily*, p. 16.
- Nolan & McFarlan, (2005). Information Technology and the Board of Directors. *Havard Business Review*, R0510F, 1-12.
- OECD (2009). *Computer Viruses and Other Malicious Software*, Author
- Olowu, D. (2009). Cyber-Crimes and the Boundaries of Domestic Legal Responses: Case for an Inclusionary Framework for Africa. *Journal of Information, Law & Technology (JILT)*, Retrieved from http://go.warwick.ac.uk/jilt/2009_1/olowu
- Panko, R. J. (2010). *Corporate Computer and Network Security*. (2nd Ed.). Pearson hall.
- Pathak, J. (2004). A Conceptual Risk Framework for Internal Auditing in E-Commerce. *Managerial Auditing Journal*, 19 (4) 556 – 564.
- Pfleeger, C.P. & Pfleeger, S.L. (2007). *Security in Computing* (4th Ed.). Prentice hall.
- PwC (2011). *Cybercrime: Protecting Against the Growing Threat- Global Economic Survey 2011*. Author.
- Rudasill, L. & Moyer, J. (2004). Cyber-Security, Cyber-Attack, and the Development of Governmental Response: The Librarian's View. *New Library World*, 105 (7), 248 – 55.
- Rutkowski, A. (2011). Public International Law of The International Telecommunication Instruments: Cyber security Treaty Provisions since 1850. *Info*, 13 (1), 13 – 31.
- Saini, H., Rao, Y.S. & Panda, T.C. (2012). Cyber-Crimes and Their Impacts: A Review. *International Journal of Engineering Research and Applications*, 2(2), 202-209.
- Salifu, A. (2008). The Impact of Internet Crime on Development. *Journal of Financial Crime*, 15 (4), 432 – 443.
- Schuessler, J. H. (2009). *GDT: Assessing Information Systems Security Effectiveness in Large versus small Businesses*. University of North Texas.
- Sherstobitoff, R. (2008). Anatomy of a Data Breach. *Information Security Journal: A Global Perspective*. 17 (5-6), 247-252.

- Smith, A.D. (2004). E-Security Issues and Policy Development in An Information-Sharing and Networked Environment. *Aslib Proceedings*, 56 (5), 272-285.
- Smith, A.D & Rupp, W.T. (2002). Issues in Cyber Security; Understanding Risks Associated With Hackers/Crackers. *Information Management & Computer Security*, 10 (4), 178 – 183.
- Solms,V. B. & Solms, V.R. (2004). The 10 Deadly Sins of Information Security Management. *Computer & Security*, 23, 371-6.
- Stallings, W. & Brown, L. (2008). *Principles and Practice of Computer Security*. Pearsons Hall.
- Stallings, W. (2006). *Cryptography and Network Security*(4th Ed.). Pearson Prentice Hall.
- Sund, C. (2007). Towards an International Road-Map for Cyber Security. *Online Information Review*, 31 (5) 566 – 582.
- Systems Administration Networking and Security Institute (2012). Retrieved on 23 September 2012 from www.sans.org.
- Trim, P.R.J. (2005). Managing Computer Security Issues: Preventing and Limiting Future Threats and Disasters. *Disaster Prevention and Management*, 14 (4),493–505.
- Tsohou,A., Kokolakis,S., Lambrinoudakis,C. & Gritzalis, S. (2010). A Security Standards' Framework to Facilitate Best Practices' Awareness and Conformity. *Information Management & Computer Security*, 18 (5), 350 – 365.
- Vanderwerken, J. & Ubell, R. (2011, February 20). Training on the Cyber Security Frontlines. *T & D Magazine*, 23 (6), 12-18.
- Volonino, L. & Robinson,S. R. (2004). *Principles and Practice of Information Security*. Pearson Prentice Hall.
- Warfield, D. (2012). Critical Infrastructures: IT Security and Threats from Private Sector Ownership. *Information Security Journal: A Global Perspective*, 21 (3), 127-136.
- Willison,R. (2006). Understanding the Offender/Environment Dynamic for Computer Crimes. *Information Technology & People*, 19 (2), 170 – 186.

World Bank (2012) *Information and Communications for Development 2012: Maximizing Mobile*. Author.

Yin, R.K. (2003). *Case Study Research: Design and Methods* (3rd Ed.). Stage Publication.

APPENDIX 1: Introduction Letter

Strathmore University

20th, December 2012

To whom it may concern

RE: Onwong'a Celestine Moige. No: 067182:

Celestine Onwong'a is a postgraduate student in our Master of Commerce (MCom) Programme in partial fulfilment of the MCom degree, students are required to carry out a research project and write a thesis on a contemporary subject within their field of specialization. Among other activities, the project involves data collection and analysis.

Ms. Onwong'a is requesting to gather information to be used in her research. The information she will obtain from your organization will be used for academic purpose only and will be kept confidential. The results of the survey will be in summary form and will not disclose any individual, organization name or organization information in any way.

The research study is entitled: "Business reactions to cyber security threats in the Kenya business environment".

We hope that your organization can assist by providing information to the above named student.

Yours faithfully,

Josphat Manani,

MCom Administrator,

School of Management and Commerce

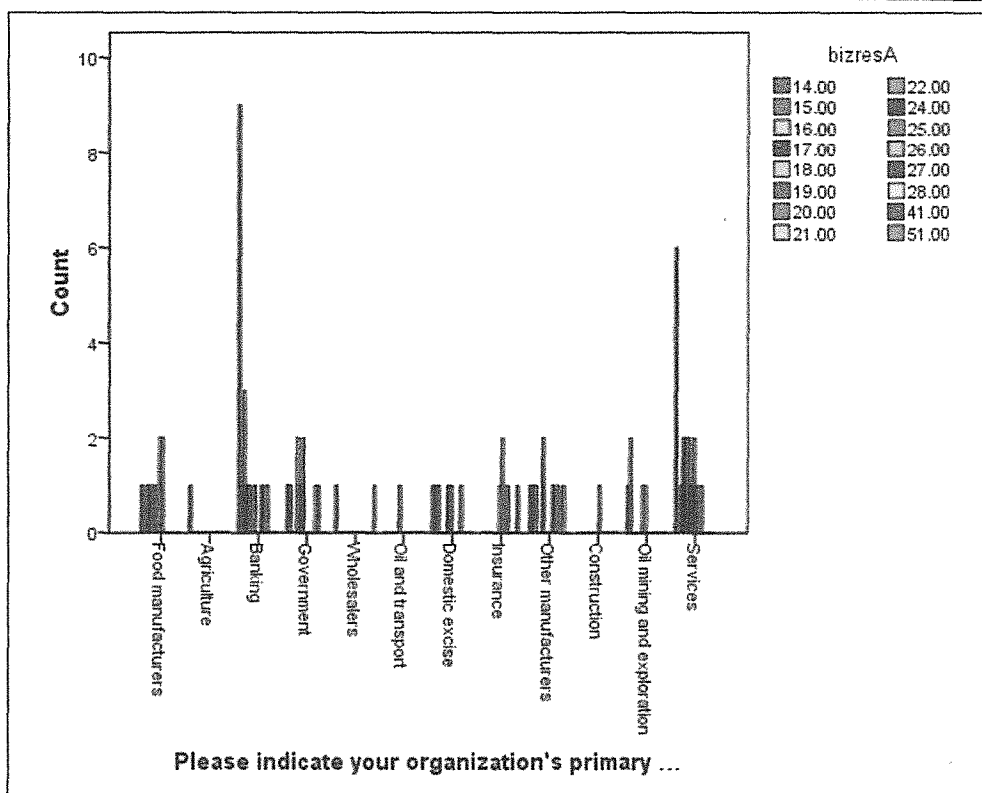
APPENDIX 2: Respondents' Sector Distribution

	Frequency	Percent	Valid Percent	Cumulative Percent
Food manufacturers	8	9.6	9.6	9.6
Agriculture	1	1.2	1.2	10.8
Banking	19	22.9	22.9	33.7
Government	9	10.8	10.8	44.6
Wholesalers	2	2.4	2.4	47.0
Oil and transport	1	1.2	1.2	48.2
Domestic excise	6	7.2	7.2	55.4
Insurance	5	6.0	6.0	61.4
Other manufacturers	8	9.6	9.6	71.1
Construction	1	1.2	1.2	72.3
Oil mining and exploration	5	6.0	6.0	78.3
Services	18	21.7	21.7	100.0
Total	83	100.0	100.0	

APPENDIX 3: Frequency of Occurrence of Cyber Security Threats

Form Of Cyber Crime	Very frequent (after two weeks)	Frequent (monthly)	Average (quarterly)	Rare (annually)	Never	Total
Malware	30.5	29.3	17.7	16.5	4.8	98.8
Cyber laundering	9.6	6.0	26.5	36.1	21.7	100
Smurfing	8.4	7.2	26.5	37.3	20.5	100
Denial of service	12.0	10.8	15.7	38.6	22.9	100
Advance fee fraud	7.2	10.8	13.3	37.3	31.3	100
Cyber squatting	10.8	4.8	12.0	38.6	33.7	100
Encryption	8.4	19.6	9.6	32.2	30.1	100
Phishing	9.6	17.2	25.3	26.1	21.7	100
Data interference	18.4	24.5	14.1	20.1	22.9	100
Botnets	9.6	18.4	26.5	21.3	24.1	100
System interference	7.2	24.5	24.1	18.9	25.3	100
Libel	10.8	10.8	21.7	27.7	28.9	100
Spam	31.3	18.1	18.1	19.3	13.3	100
Eaves dropping	19.3	12.0	16.9	22.9	28.9	100
Copyright piracy	18.1	13.3	19.3	19.3	30.1	100
Malicious code	25.7	18.4	14.5	26.1	15.1	100
Identity theft	30.8	13.3	12.0	26.1	17.7	100
IP Spoofing	8.4	22.0	18.1	22.5	28.5	100
Vishing	10.8	8.4	18.1	28.9	33.7	100
Cyber espionage	9.6	7.2	13.3	31.3	38.6	100

APPENDIX 4: Business Reactions as Relates to Different Sectors



APPENDIX 5: Questionnaire

PART A: BACKGROUND INFORMATION

Respondent's name (optional) _____					
Job description					
IT		Internal auditors		Others (specify)	
For how long have you been working in your organization					
Less than 5 yrs		5-10 yrs		11-15 yrs	
16-20yrs		Over 20 yrs			
Please indicate your organization's primary industry affiliation (multiple selections)					
Food manufacturers		Agriculture		Banking	
Government		Wholesalers		Oil and transport	
Domestic excise		Insurance		Other manufacturers	
Construction		Oil mining and exploration		Services	

PART B: CYBER SECURITY THREATS AND CHALLENGES

I: Cyber security awareness in your organization:

1. Have you had cyber security issues in your organization?
 - (a) Yes (b) No (c) Not sure
2. Does your organization have an information security plan in place?
 - (a) Yes (b) No (c) Not sure
3. What portion of your IT budget is spent on IT security?
 - (a) Less than 3%
 - (b) 4%-7%
 - (c) 8%-10%
 - (d) More than 10%
 - (e) Unknown
4. How do you rate your organization's implementation of cyber-space security?
 - a) High (b) Moderate (c) Low

5. Do you have in place cyber security strategies within your organization?
(a) Yes (b) No (c) Not sure
6. Are the cyber-space security strategies in your organization consistent with the
cyber- space demands for internal and external environment?
(a) Yes (b) No (c) Not sure
7. Are the cyber-space strategies in your organization consistent with the
expectations of the CCK?
(a) Yes (b) No (c) Not sure
8. The cyber security function is primarily viewed as:
 - a) An administrative job focused on granting user access and establishing degrees of privilege
 - b) Critical to the long-term survival of the organization with emphasis on maintaining relationships with employees, business partners and government regulators.
 - c) Technically oriented with an emphasis on addressing authentication and authorization issues and maintaining physical security of computer resources.
 - d) As a resource to maintain compliance with information security standards and best practices.
9. What is the composition of the information security team? (Please tick)
 - (a) IT staff
 - (b) Internal auditors
 - (c) Middle level managers
 - (d) Top managers
 - (e) Others (specify)
10. Please indicate the frequency of top management's participation in information
security planning:
 - (a) Almost always

- (b) Frequent
- (c) Infrequent
- (d) Seldom

II: Cyber security threats' characteristics

11. Do you agree or disagree with the following statements:

a) Cyber security threats are generally characterized as borderless i.e. cyber attackers and cyber victims seem to be located anywhere in the world. (Please tick one)

Strongly disagree 1	2	3	4	Strongly agree 5

b) Cyber security threats are generally characterized as having unobserved ethical boundaries i.e. ethical boundaries are not observed as people tend to ignore ethics in the cyber world. (Please tick one).

Strongly disagree 1	2	3	4	Strongly agree 5

c) In case where a cyber security threat has occurred, it is generally difficult to establish the persons responsible. (Please tick one).

Strongly disagree 1	2	3	4	Strongly agree 5

d) Cyber security threats are generally characterized as having multiple effects i.e. automation enables a criminal to plant an attack and leave it to multiply itself at very fast rate and with minimal human intervention. (Please tick one)

Strongly disagree 1	2	3	4	Strongly agree 5

e) In case where a cyber security threat has occurred, it is generally difficult to prosecute offenders. (Please tick one).

Strongly disagree 1	2	3	4	Strongly agree 5

f) Cyber security threats are generally characterized as requiring low cost in actualizing them. (Please tick one).

Strongly disagree 1	2	3	4	Strongly agree 5

g) After their occurrence, cyber security threats are generally less reported than normal crimes. (Please tick one).

Strongly disagree 1	2	3	4	Strongly agree 5

h) Cyber security threats are generally characterized by anonymity. (Please tick one).

Strongly disagree 1	2	3	4	Strongly agree 5

11. In your opinion what makes cyber security threats to spread so rampantly?

Characteristic	Strongly agree	agree	uncertain	disagree	Strongly disagree
Borderlessness					
Unobserved ethical boundaries					
Difficulty in establishing person responsible					
Difficulty in prosecuting					

offenders					
Threats have a multiplier effect					
Low cost					
Few reported cases					
Anonymity					

III: Manifestation of cyber security threats

12. On a scale of 1-5 where 1 is for strongly disagree and 5 strongly agree, how would you rate the following statements as regards various cyber security threats?

Cyber threat	Statement	1	2	3	4	5
Malware	a) Malware threat is easy to deter					
	b) Malware threat is easy to detect					
	c) Malware threat is easy to prevent					
Cyber laundering	a) Cyber laundering threat is easy to deter					
	b) Cyber laundering threat is easy to detect					
	c) Cyber laundering threat is easy to prevent					
Denial of service	a) Denial of service threat is easy to deter					
	b) Denial of service threat is easy to detect					
	c) Denial of service threat is easy to prevent					
Phishing	a) Phishing threat is easy to deter					
	b) Phishing threat is easy to detect					
	c) Phishing threat is easy to prevent					

Identity theft	a) Identity theft is easy to deter						
	b) Identity theft is easy to detect						
	c) Identity theft is easy to prevent						
System interference	a) System interference threat is easy to deter						
	b) System interference threats is easy to detect						
	c) System interference threat is easy to prevent						

13. On a scale of 1-5 where 1 is for strongly disagree and 5 strongly agree, how would you rate the following statements? On the manifestation of cyber security threats, the following effects would be experienced:

Effects of manifested cyber security threats	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Deletion of system files					
Corruption of files and folders					
Denied access to files					
Forwarding of confidential information					
Loss of customers					
Loss of reputation					
Loss of staff morale					

Declined profitability					
Increase in Legal costs					
Loss of competitive advantage					
Loss of investors					

IV: Business reactions to cyber security threats:

14. Do you agree or disagree that your company has embraced the following technical countermeasures to curb cybercrime?

MEASURE	YES	NO	I DON'T KNOW
Anti-spam filter technology			
Anti-piracy			
Anti-jam			
Anti-spoof			
Anti-spyware			
Honey-pot			
Data back-up systems			
Password			
Anti-virus software			
Encryption			
User authentication			
Digital signatures			
Firewall			
Patch			

15. Do you agree or disagree that your company has embraced the following non-technical countermeasures to curb cybercrime?

MEASURE	Yes	No	I don't know
An operational cyber security policy document			
You have instituted best practice standards			
There is an existence of contingency plan			
There is regular IT security training on the users			
Audit of various system logs is carried out			
Encourage security violation reporting			
Has a management framework to initiate and control implementation of IS security			
There is a plan for various contingencies			
you work with external legal and regulatory entities to enforce and protect the organization's interests			
Has scheduled, periodic reviews of the information systems security policy			
Reinforces information security responsibilities to employees throughout their career			
Has a formal reporting procedure for identified security incidents and weaknesses			
Has a formal policy to protect against risks associated with obtaining files from unauthorized sources			
Has established incident management procedures for information system security incidents			

THANKYOU!