AN ASSESSMENT OF SECURITY MEASURES FOR ELECTRONIC INFORMATION RESOURCES IN SELECTED ORGANIZATIONS IN NAIROBI.

WEKALAO BEN NAMAANDE

A PROJECT REPORT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF MASTER OF EDUCATION, LIBRARY AND INFORMATION STUDIES, SCHOOL OF EDUCATION, KENYATTA UNIVERSITY.

DECLARATION

This dissertation is my original work and has not been submitted for the award of a similar qualification in any other university.

.....

Wekalao Ben Namaande.

This dissertation has been submitted for examination with my approval as a university supervisor.

.....

Mwathi, P.G.

DEDICATION

This dissertation is dedicated to my loving wife; Everlyn Nafula, dear children; Ian, Wayne, Owen, Wendy, my caring grandmother, Dorcas, and to the memory of my late brother in-law (Alfred Simiyu) who heralded my research endeavours, for their love and support, and their strong faith in the power of knowledge.

ACKNOWLEDGEMENTS.

I'm grateful to the Almighty God for having made the study a reality. Many are times that I thought I would never go through due to the many forces that militated against my studies. However, since all things are possible with God, my vision of getting a Masters degree against all odds and expectations materialized.

This dissertation is a result of my own independent research. However, while I take full responsibility for the views expressed in it, I would like to thank individually and severally, many a people and institutions for their support, which made it possible for me to complete my studies. I particularly appreciate my supervisor, Mr. P.G. Mwathi who was always available for me and read through several drafts of this work beginning from the proposal level. His guidance greatly contributed to the richness of this study.

It will be a disservice for me to overlook the input of other members of the world of academia. Mr. E. Waiguru Muya's efforts to push me to the cutting edge of knowledge and its frontier expansion cannot go unappreciated. Others from whom I greatly reaped knowledge include Mr. Njuguna JR, Mr. Mukuvi, Ms. Mathu, Mr. Thuku and Dr. Kaane. My gratitude also goes to my sister in-

law Everlyn Wataka who typed the final chapter of this document and many other corrections. To the secretarial staff Elizabeth and Wambui, thank you!

I would also like to thank all my respondents for their cooperation, which made my field work a worthwhile experience. Special thanks to my friend, Eliakim Azangu for his several inputs and guidance in producing this report. The entire study could have been boring without the company of my colleagues; Catherine Muriuki, Lilian Karanja, Emily Wanjohi and Rachael Kagoiya, and, a semester later, Horo and Munyoki.

This study could not have been possible without the support of my family. I acknowledge with gratitude the love, tolerance and patience of my wife Evelyn Nafula, throughout the period of study. My encouraging and inspiring sons Ian, Wayne, Owen and daughter, Wendy are highly appreciated. Special thanks to the following who made immense financial investments in my entire education cycle: Kukhu Dorcas, Kuka Namaande, Uncles Paul, Nelson and Aunts Jessica and Bilhiah.

I also appreciate the DPM (Department of Personnel Management) and my employer, Kenya National Archives and Documentation Service, and by extension, the Ministry of Home Affairs for allowing and financing my studies.

Although many people made an input in my studies, I would like to appreciate, albeit posthumously the personal efforts of my late brother in-law and friend, Alfred Simiyu Munyekenye who baby walked me in the initial stages of my research especially proposal development, just before his life was cruelly and crudely robbed out of him by the Nairobi thugs. May the Almighty God rest his soul in eternal peace.

For everybody who contributed to the success of this study, thank you severally and individually.

ABSTRACT

The purpose of this study was to assess security measures in place for electronic information and its infrastructure in selected organizations in Nairobi. The main objectives for the study were: establishment of the status of current security measures for electronic information systems in selected organizations in Nairobi, to suggest a possible security policy for organizations dealing with Information Communication Technology and to identify possible solutions to the problems. Before assessing the measures, the researcher identified some specific threats that electronic information faces. The study found out that electronic information and infrastructure faces two broad types of threats: physical and logical.

Physical threats are the vulnerabilities militating against electronic information because of physical weaknesses such as improper securing of the information facilities. Measures for this brand of threats are also physical e.g. construction of bomb proof buildings, keeping out of bounds any unauthorized personnel in and around the information communication technology main center, and 24 hour round the clock surveillance, etc.

On the other hand, logical threats are system-oriented dangers, which cripple the operations of the information system. As technology stands today, anybody with a computer and a modem can have access to the Internet or the WWW, however, not everybody surfing the web has good intentions. Some are driven by ulterior motives such as stealing or destroying information.

Others simply enjoy making the information systems in-operational through developing deadly viruses and or programs whereas other Internet users treasure infiltrating other peoples sites and addresses filling them with dirty literature or junk messages that any civilized society will frown upon.

The study concludes that electronic information systems are crucial in the networked world. However, since they are faced with myriad security problems that cannot be overlooked, organizations are called upon to develop and implement programs that are geared towards achieving total security of the information resources.

It is against the understanding of some of these electronic information bottlenecks that measures and or security policies can be formulated to address the threats. Physical security can be achieved through restricted access to the computer systems, burglarproof storage facilities and backups among others. For logical security, user IDs and passwords, enactment and enforcement of laws to deter cyber crimes and Information classification etc. are recommended as security measures. The measures and or recommendations pointed out in this study, if well adhered to, can be of value to electronic information security.

The study was carried out in two types of organizations in Nairobi. They were mainly public and private. The two types were further categorized into several categories based on their functions in society. They were categorized thus as

Financial, Communications, Research, Academic/Training and Information Centers/Libraries.

For each of the type and category of organization, three questionnaires were developed and administered. The first questionnaire was tailored for the information communication technology (ICT) specialists. The second questionnaire was developed with the ICT user in mind (regardless of whether or not one is a staff member of the organization). The final questionnaire addressed the ICT vendors. The three questionnaires are thus the foundation of the three parts of data analysis and interpretation in chapter four. The actual study was preceded by pre-testing questionnaires to ascertain their suitability to generate data from respondents. The questionnaires were then administered, interview with key informants carried out and observations made to generate data for the study. The data collected was then qualitatively analyzed, discussed, and then conclusions and recommendations made.

TABLE OF CONTENTS

CHAPTER FIVE: Summary of the main findings, conclusions and Recommendations..... 112

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ATM	-	Automated Teller Machine
AIU	-	Alliant International University.
AP	-	Associated Press
CD	-	Compact Disk
CD ROM	-	Compact Disk Read Only Memory
COMMLA	-	Commonwealth Library Association
D.O.S	-	Denial Of Service
DPM	-	Directorate of Personnel Management
DVD	-	Digital Visual Display
FBI	-	Federal Bureau of Investigation
GTI	-	Gilgil Telecommunications Institute
ICA	-	International Council on Archives
ICT	-	Information Communication Technology
ID	-	Identification Number
IFLA	-	International Federation of Library Associations and Institutions
IP	-	Internet Packet
ISP	-	Internet Service Provider
JKUAT	-	Jomo Kenyatta University of Agriculture and Technology
KASNEB	-	Kenya Accountants and Secretarial National Examination Board

KBC	-	Kenya Broadcasting Corporation
KCCT	-	Kenya College of Communication Technology
KIPS	-	Kenya Information Preservation Society
KLA	-	Kenya Library Association
KUSCO	-	Kenya Union of Corporative Societies
NASA	-	National Aeronautical and Space Agency
NY	-	New York
PABX	-	Private Automatic Branch Exchange
PC	-	Personal computer
PIN	-	Personal Identification Number
SCECSAL	-	Standing Conference of Eastern Central and Southern Africa Libraries
SSL	-	Secure Society Layer
SPSS	-	Computer Package for Social Science
UON	-	University of Nairobi
URL	-	Uniform Resource Locater
URTNA	-	Union of Radio and Television Network in Africa.
USIU	-	United States International University
VCR	-	Video Cassette Recorder

CHAPTER ONE

Introduction

In this chapter, background to the study, an outline of the problem, aim, objectives, research questions and significance of the study are discussed. The background study gives a brief history and /or origins of information in conventional formats and transition to electronic formats while at the same time contrasting the then security cum storage devices to the situation pertaining to current electronic formats. The outline of the problem simply states the problem, aim echoes the goal of study, objectives are what the study aims to achieve, research questions are parameters for generating data, while significance of the study is the importance or justification for the study.

1.1 Background to the study

Organized information storage began with the invention of writing. In the early days, it was in the form of clay tablets, papyrus and leather scrolls. With the discovery of printing, a lot more information could be stored on documents, thus precipitating widespread reading habits. This created the need for libraries where this information could be conveniently stored and accessed by users. These resources comprise books and journals among others.

The discovery of computers made it possible for information to be stored in digital or electronic formats thus allowing a large amount of information to be stored in a relatively small space. This form of storage of information has now permeated almost all sectors of

society. Electronic information therefore is information that can be manipulated, transmitted or processed by a computer. It is written on non-book media such as magnetic tapes, cassettes, CD ROMS, hard disks and diskettes using computer software and hardware. The invention of networks and the Internet made it possible for such information to be shared between computer users. However, the massive gains brought by Information Age are not perfect. The technological development brought with it a number of security related problems.

According to Gehring, R (2003.1) at http://elj.warwick.ac.uk/jilt/03, security is the property of a system to resist unauthorized access to and use of the system's resources, the opposite of which is insecurity i.e. vulnerability. With the pervasive correlation of human activity with electronic resources and infrastructure comes vulnerability- the ever-present risk of abuse, insidious manipulation and sabotage of computers and computer networks. On several occasions the world has witnessed electronic attacks of catastrophic proportions. January 2003, for instance, saw the strike of the infamous slammer worm (see Section on Logical/systems Security in the Literature Review).

Though traditional or conventional sources of information are used concurrently with electronic sources in most institutions, security measures for the conventional sources are fairly developed. Some organizations use closed access system as a security measure, others do not lend out their documents, in most, if not all organizations, bags and overcoats are prohibited in the reading areas and, publications from outside are not allowed into the information organizations. In well-developed information organizations,

closed circuit monitoring systems are in place to provide round the clock surveillance. In addition, electronic chips are applied to library materials in order to foil any attempt to illegally channel information resources outside the organization concerned. However numerous problems arise when handling electronic information. These include fragility of storage devices such as diskettes, rapid technological development also means such devices become quickly obsolete. It therefore becomes difficult to retrieve stored information therein because storage and retrieval systems become incompatible. Where information is carried between computers, it is prone to deliberate malicious threats. The internet also opens up a wide range of opportunities for tampering with such information. Even where infringements occur, it is difficult to trace these where qualified personnel are lacking. Since electronic information is in digital form, protection is usually in the form of logical means rather than physical methods. Some examples to curb this include restricting access to computers, use of passwords and encryption. While these are known from general literature, few institutions have them in place.

1.2 Statement of the Problem

Over the years the data processing user has been primarily concerned with the integrity of his data. Integrity is the representation of information and the transformation of information without errors. Where information between computers in a networked environment is prone to deliberate malicious threats, protection is assured by logical means rather than physical methods.

Electronic information security is about protecting one's data from the myriad threats via the Internet. As technology stands today, anybody with a computer and a modem can

access the Internet. However not everybody accessing the internet has good intentions and neither are all websites on the internet built with good intentions.

Security for electronic information is of great importance to any organization or government. The importance of information security takes an added meaning because of increased threats to the systems and information they store, process, and transmit due to expanded connectivity. Every day, computer crimes are committed in the world, across cities, countries and continents. Problems such as leakage, hacking, alteration and removal of information interfere with, and or, compromise both the integrity and confidentiality of information and its physical form. Where security is compromised, it is not always easy to look at an affected computer and tell what occurred. Security for electronic information is a fairly new concept in developing countries such as Kenya. While appreciable measures are usually in place in private institutions such as banks, very little exist in public institutions.

1.3 Aim of the study

The goal of this study is to assess the status of current security measures for electronic information in a sample of organizations in Nairobi where permission was granted. These comprise information centers, financial institutions, communication organizations and the Government Computer Service (GIS). It is therefore necessary to evaluate the measures, if any, which are in place to safeguard such information for the present and future.

1.4 Objectives of the study

2. To establish the status of current security measures for electronic information systems in the organizations under study.
2. To identify specific threats to existing electronic resources at the organizations and identify possible solutions to the identified problems.
3. To suggest a possible security policy for organizations dealing with Information Communication Technology.

1.5 Research questions

1. What ICT facilities are utilized in your organizations?
2. Are they secured? What are the threats facing the ICTs in your organization?
3. What are the possible solutions to the threats?
4. What should be the policy for security of electronic information resources?

1.6 Conceptual framework

This is a hypothesized model of identifying the concepts under study and their relationship. The purpose is to help the reader to quickly see the proposed relationships. The following concepts as used in the topic and elsewhere in the study are worthy explaining albeit in brief: assessment, security of electronic information resources and threats.

Assessment

In this study, "assessment" is a concept that captures my research goal, objectives and activities in a condensed format. It represents a collection of activities that were crucial to generation of data for my study. They include finding out:

- types and categories of organizations studied,
- ICT facilities in use at the organizations under study,
- risks or threats to ICTs in these organizations,
- if the organizations have any security measures in place and variations in levels of security
-

Security of electronic information resources

Security refers to the property of a system to resist unauthorized entry or destruction. Electronic information is information that is transmitted electronically and it is differentiated from other forms of information in the manner in which it is accessed (through computerized settings). This is the latest version of information storage and, unlike conventional information sources, electronic information cannot be locked up in cabinets or stores. Since some organizational information is considered too confidential to be tampered with or lost, some security measures such as PIN, passwords, restricted access, backups etc. are put in place. They are these security measures among others developed by the organizations under study that the research is all about.

Threats

Electronic information security measures are not an end in themselves. They can be compromised or tampered with. This constitutes a threat to electronic information. Organizations, therefore, are faced with the challenge of continued development of security measures to safeguard their electronic resources from threats.

1.7 Significance of the study

Most electronic devices are usually expensive to stock and quickly get out of date. They therefore become very vulnerable to security threats, particularly where funds for updating these are severely limited as is the case in many local organizations. Information sent via Internet is not secure. It is possible that some one else can steal any information you send without you knowing about it. It is therefore necessary to know how best to secure electronic information. The concept of security of electronic information is not extensively embraced in our local scene. As an example, it was not until 2003 that the necessary legislation for Electronic Communications and Transactions Bill was drafted and enacted into law in Kenya. The Bill provided for an Act of Parliament to provide for legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication commonly known as "electronic commerce", which involve the use of alternatives to paper based methods of communication and storage of information; to legalize electronic delivery of services by the government; to protect privacy of individuals and interests of consumers of Information technology services among other stipulations. The Bill became what is known as the "Electronic Transactions and Electronic Communications Act, 2003". Even

so, to date, Kenya does not have adequate legislation to protect corporations and individuals from information technology and communication related crimes. This study presents an assessment of security situations for electronic data and makes possible recommendations for security enhancement. It discusses what should be done to protect information systems. In assessing the effectiveness of current security measures in local organizations, it is expected that this study will provide an example for managers in these organizations to evaluate their own security measures and initiate, coordinate and implement security policies for their respective electronic information. It sets out to identify some of the threats facing electronic data and pinpoint possible measures employed to secure data from the perceived threats. It will therefore hopefully provide a baseline from which improvements can be made. Since the methodology is standardized, the evaluation can be used across the whole spectrum of organizations.

The issue of data and information security is important to ensure that any information relayed is not secretly copied by wiretap or other means and diverted to other destinations. This calls for measures to be put in place to address the whole set of computer crimes such as illegal programs, malicious logic bombs and viruses that may make systems inoperative once they are executed leading to massive loss of data and information from the organization's electronic network system.

Thus the underlying justification to undertake the study was the need to add to or expand the frontiers of knowledge as regards the field of Information Communications Technology. Secondly, though there is a considerable number of studies done on security

of electronic Information, there is a research gap that needs bridging as none whatsoever has been done about our local environment. Whatever has been done is on general ICT issues but this study is basically on what constitutes measures to combat threats to electronic information and or create awareness on the need to be disaster and recovery prepared in case of an eventuality.

Thirdly, since the world economies are now pegged on Information Communication Technology, the Nairobi ICT users cannot afford to operate without knowing the threats that their daily companion (ICT) faces and the antidote for the same, hence my attempt to examine and offer solutions to the problems through the findings in this study. It is also hoped that this study will provide a baseline for future researchers to investigate this problem further.

CHAPTER TWO

Literature Review

This chapter presents a review of related literature and provides the needed support to the researcher's rationale for undertaking this study. Much of the literature on ICT security has been systematically analyzed to identify the missing gap i.e. Despite the many studies, the review established that no study has been undertaken on security of information systems in Nairobi, hence the justification for this study. In this chapter, a review of what others have done in ICT security has been done. The pattern of review is tailored along the goal and objectives of the study. As already pointed out in the preliminary information, the goal of this study is to assess the status of current security measures for electronic information in a sample of organizations in Nairobi where permission was granted. The main objectives are establishing the status of current security measures for electronic information, identify threats facing security of electronic information and suggest a possible security policy and solutions to the problems. This chapter also systematically attempts to answer the research questions of the study. The pertinent research questions that the review is pegged on include:

- What are the threats facing electronic information systems?
- What is the status of current security systems?
- What are the possible solutions to these threats?
- What should be the policy for security of electronic information resources?

2.1. General overview

Before the dawn of information communication technology, security focus was on conventional or physical sources of information such as books and serials among others. The traditional librarian employed the following security measures that are still compatible with the electronic world: installation of electronic bugs, exit security systems, perimeter and sonic alarms, lock down devices to secure equipment and electronic surveillance cameras.

However, the emergence of Information Communication Technology in the later part of the 20th and the dawn of the 21st centuries brought with it new trends in information provision and consumption. With the Internet, libraries and other information organizations became part of the cyberspace with far reaching implications on security. In the cyberspace (a place out there), people exchange news, talk or chat with one another, commit crimes, make love, plot wars, alter information and damage information disseminating components (computer hardware and software).

It is against this backdrop that Mutonyi (2003.16), asserted,

> The 21st C. information scientists are confronted with many security related issues even as they migrate and emulate digital formats. As the book stock in the library continue to diminish, the new generation librarians have to retool themselves to be able to deal with a clientele that is becoming more and more impatient and a chaotic cyber world that is proving difficult to manage as by the second, preservation and security issues become even more complex. The ubiquitous nature of the cyber world where digital data is available globally to users complicates preservation and security even further.

It can rightly be argued that a great number of people access the Internet with ulterior motives. Some want to steal information; others want to destroy certain or any information they come across. In support of this argument, Onunga (1998:193) states,

> A rival company can break into your company's system and steal tens of thousands of dollars, as well as trading secrets. Reports estimate that every year companies in the U.S. loses about 5 billion dollars because of people breaking into their systems.

Thus there is need for extra care when handling information communication technology and the information transmitted thereof. As computers take on larger and larger share of business transactions, the need for data security becomes evident. Hardly a correspondence, a cheque or even invoice is written today by medium sized to large corporations without the assistance of computers. According to Pursur (1993.123), it was standard practice twenty years ago for clerks in accounting departments to keep financial records locked away for security reasons. But today's computer users utilize special passwords to "lock up" important information since information security is quite essential for the integrity and credibility of information. From the above, Pursur (1993:123) underscores the importance of security to shield both paper and computer based information from the super highway marauders and vandals.

In support of the above, Kovacich (1998:ix) argues,

> the coming of the age of computer and telecommunication high tech systems added a new dimension to security management as no system seems to be free from hackers, crackers .....

Storage of information electronically has however, numerous advantages. The most obvious is that it becomes possible to store extremely large quantities of information in a

relatively small place. It too has its own disadvantages related to retrieval. Despite the advantages, digital information needs customized software and hardware to retrieve. According to the *Nation,* January 22nd (2003), files may survive in the long run but the equipment to make sense of them does not. Thus technological obsolescence is a serious problem considering that technology is not static.

To Marnoff (2000:857), electronic information can be pasted, reassembled and transmitted effortlessly online, it is inherently unstable and vulnerable to loss of intellectual content. Simply put, due to the fact that many people of the 21st century are technologically literate, electronic information is an endangered species as majority of the users of information systems cannot be trusted. Some users genuinely seek information from the network and or use information technology facilities responsibly. However, others simply use the facilities to commit computer crimes such as intentional disabling of the system and or complete vandalizing of computer equipments in use.

Some form of restriction of access to such information needs to be in place because most of what is stored is of confidential nature to the concerned institution, business or government. For example, according to the U.S.A's National Aeronautics and Space Agency (NASA) IT security program (2000.23), NASA handles all the information related to the United States government's space program policies, both civilian and military, which by its nature, is highly confidential. As such, its Procedures and Guidelines Policy sets out an elaborate set of procedures that are meant to safeguard its Information Communication Technology (ICT) resources. It encompasses IT security management, planning, implementation, and performance evaluation.

2.2 Some specific threats facing electronic data.

2. 3 Logical or systems threats

Whenever a company or an individual is connected to Internet, there is exposure to security threats. Insecurity problems on the Internet emanate from the technology used for accessing the Internet. Schweitzer (2003. 216 a) defines "threat" as "any circumstance or event with the potential to cause harm to an organization through modification or destruction of information or denial of service (D.O.S)." Compared to physical information, threats to electronic information are highly complex. Schweizer notes that nearly any code that can be run on a personal computer can be manipulated towards malevolent action. He gives a comprehensive review of threats to electronic information. This includes data corruption, theft, and loss of productivity, inappropriate content, espionage and sabotage.

To the above, Pursur (1993.6) adds leakage, impersonation, masqueration and repudiation. These threats are magnified where computers are networked. A networked environment allows information resource sharing, which, though an advantage encourages quick spread of viruses which infect many systems before being detected. Related threats to networks include misrouting of traffic and malicious unavailability of network services (Artificial Network Jamming). This category of threats is directed more at the infrastructure than user information. Miller (2000.645) states that the internet, which has largely replaced local area networks for simultaneous access of information by several users, was not available to the librarians until the early 90s and by the late 90s it was almost impossible to be ignored. Thus its applications in library and information

services opened up wide ranging opportunities for tampering with information. Gerald (2000.9) seems to agree with Miller when he states,

> the coming of computer age and telecommunication high tech systems adds a completely new dimension to information system security.

The importance of Gerald's statement is that Information Communication Technology has complicated matters of data security due to the ability of cyber thugs to keep themselves abreast of technological innovations. Schweitzer (2002.216) concurs with Gerald. He is of the view that the most serious threats to electronic information arise as a consequence of the all-too-familiar viruses and worms that exploit Internet based services such as email and chat rooms. These are tiny man-made programs that attach themselves to another program to ensure that they are executed. They inflict damage on electronic information by destroying or altering existing data and sometimes adding unnecessary data.

Thus in today's wireless world, confidential data is stored and transmitted online, hence increasing its vulnerability to harm through viruses. Some, such as the Trojan Horse, are used by hackers to scan and hijack personal computers, vandalize and deface websites (British Broadcasting Corporation, 22nd July 2003). Onunga (1998.195) agrees with the foregoing over the threats. To him, there are several common threats posed by using Web browsers and their enhancement features such as programming tools and plug ins. These include privacy violations, malicious programs, and interception of sensitive or confidential information, and forged or redirected information.

Privacy violation is the common threat faced by users. This is the acquisition by the third parties of personal information on freely given data i.e. web services collect network address and computer name, user movement on site, e-mail address and other files on the user's computer which may be read or copied to a remote system. On the other hand malicious programs are security related software bags that allow malicious web based programs to damage or compromise networked computers. They may destroy sensitive files, and cause the browser to crash. This is what is referred to as denial of service attack. William, J. (2004:2) affirms the above,

> One of the tools used in data theft is a Trojan Horse virus. This is a program used by hackers to comb your personal computer or network for confidential data files. These malicious programs come as e- mail attachments and can compromise a system by opening a 'backdoor' entry into a computer server and can even access member passwords and credit card information.

On the same note, Pursur (1993.7) observes,

> Trojan Horses are used to deliver a damaging viral payload that at times results in denial of service. This has the consequence of productivity loss in the man-hours wasted in identifying and removing them. For business that is transacted via electronic systems, significant loss of revenue is incurred.....

According to Schweitzer (2002.217), Corporate Humiliation also arises when viral attacks are publicized. Two famous cases are the circulation of official FBI documents in 2001 and the spread of the *'Love bug'* virus using Microsoft's Operating System, which is used in the majority of computers. While these attacks are preventable, they can be quickly modified, as has been the case with the recent *Blaster* and *Sobig* series of worms (Daily Nation, August 14th 2003).

The fact that hacking and computer attacks are taken seriously was underscored by the Associated Press Report adopted by the East African Standard, July, 4th 2003 and the Sunday Nation, July 5, 2003. It states,

> An early warning network for the technology industry, operating with household security, notified companies that it received 'credible' information about the attacks and already has detected surveillance probes by hackers looking for weaknesses in corporate and government networks. Separately, the NY Cyber Security Office warned Internet providers and other organizations that the goal of the hackers is to vandalize 6000 websites in six months.

Indeed, threats to electronic facilities and information are real and organizations the world over are alert to counter them.

One other major threat to electronic information system is spamming. Spamming is the sending of unsolicited emails to multiple people who have not asked for it or multiple postings of the same or slightly altered article to many newsgroups. Thomas (1998.41) describes them as the scourge of the Internet as they not only clog it but also pose an unnecessary cost to the person downloading them.

Cyber-Terrorism is a recent serious threat to electronic systems. According to Schweitzer, Cyber Terrorism is an unlawful act that is carried out against computers in order to coerce or intimidate others. It encompasses attacks made on computer systems, networks and information stored on them with the ultimate objective of influencing a population or government to conform to a particular political, social or ideological agenda. This may result in colossal monetary losses, injuries and deaths when systems that control vital services or machines such as communications are affected.

Senator John Edwards of North Carolina made an interesting analogy between the effect of cyber terrorism and that of a deadly weapon,

> We live in a world where a terrorist can do as much damage with a keyboard and a modem as with a gun and a bomb" (Daily Nation, 22nd, Jan. 2003).

It is thus evident that the effects that logical or computer terrorism can cause to society are as damaging as those caused by physical terrorism.

Espionage is another threat to electronic data. It can be initiated and sometimes bankrolled by governments. This may be as a result of bad relations or just industrial competition. The Internet not only allows espionage to occur within an organization but also from outside. This justifies the tendency for governments and institutions to go to great lengths to invest in safeguarding their electronic resources. For example, disgruntled or former employees can cause considerable damage to an institution's electronic resources. In this regard, Steve West (2001.98) emphasizes the importance of trust and security in any online transaction to ensure that communication over a network is protected. He argues,

> The identity of both parties involved in a transaction needs to be assured before they can trade in good faith, in fact each party in the transaction will want assurance that the other party is trustworthy.

Purser (1993.125) adds confidentiality in dealing with an institution's electronic information resources. This is of particular importance when outside parties e.g. engineers are involved. These parties become a threat not just to the hard ware e.g. in case of theft, but also the software and information in a system. As an example, William,

J. (2000.249) extensively discusses a case where engineers looked at an individual's computer hard drive, when taken to them for repair, and leaked the information contained therein to the police that led to his arrest and prosecution.

Closely related to the above is 'masqueration', whereby the attacker pretends to be the legitimate host. This could be a website within a similar URL, designed to defraud a company or gather money or information in false pretence.

In the recent years, the risk of computers being attacked through emails or the Internet has risen drastically. By using the Internet and connected technologies, one gains access to the whole world and opens a world of opportunities for endangering the technology in use. Viruses, worms Trojan Horses, hackers, spy-ware, slammer worms and other kinds of intrusion are electronic threats that cannot be underestimated. They can cause computer crash to an extent of grounding organizational operations. An article titled "Analysis of Law on Cyber Crime by Ngugi Mathew in a Legal Week Magazine of the Daily Nation (7th, Feb. 2005), defines 'Slammer Worm' and articulates the devastating effects that it may cause. He explains,

> A slammer worm is a simple but versatile malicious code that, within 15 minutes of its first infection voraciously replicated itself throughout the World Wide Web disabling over a half a million cable modems, disrupting numerous flights, stalling emergency services and interrupting internet and cell phone use for over 100 million people worldwide. Estimated losses topped 80 billion Kenya shillings within a week of the ensuing mayhem.

In the Kenyan context, this observation brings to the fore questions on Kenya's ability to defend or protect her information technology in case of an attack.

On the other hand, unauthorized access may lead to theft of business secrets and new inventions of an organization. Other negative consequences of the mentioned threats comprise loss in terms of time, money, customers and data (a Symantec Operation 2004 available at www.symantec.com/uk/small business/) With regard to software, unauthorized copying of software is a risky business that can put a company in jeopardy. Conversely, proper software management cushions a company from software abuses that may include risks such as financial damages and legal costs for Copyright infringement. Abusing software may also damage a company's reputation.

Besides, unauthorized software can contain viruses with the potential to damage both individual computers and entire networks. In retrospect, they may cause irretrievable data loss that may be a devastating blow to an organization. Besides, unlicensed software may cause incompatibility programs that would normally function together seamlessly. Symantec also isolates other threats as being piracy and noncompliance related. Among them are end user copying, hard disk loading, counterfeiting, miss- channeling and Internet piracy.

Hardware obsolescence is another threat to electronic information. Rapid technological developments quickly render traditional instruments of managing high-tech crimes quickly out of date. For example, many new machines can no longer read magnetic tapes of the early form of electronic information storage. Zandonella (2002.44) in justifying the foregoing says:

> It took a modern expert a two-week course to learn how to use a 1965 Honeywell Kitchen Computer.

Problems associated with deciphering information on such storage devices would subsequently be more formidable. These sentiments are echoed in a business editorial from New York entitled "*Digital Dark Age Approaches*" published in the Daily Nation, 12th January 2002. It states:

> The computer files may survive but the equipment to make sense of them might not. This era could become a "digital dark age,"- a part of its memory forever lost. At risk are your e-mails and music and that is just for starters. Institutions meanwhile are grappling to ensure longevity of digital art, electronic court filing, Journals and much more.

To the International Records Management Trust (1999.28), the life cycle of electronic records is longer than the life cycle of the systems used to create them. According to this agency:

> Computer systems become obsolete so rapidly that it is unrealistic for these systems to remain usable for the length of time that the organization will need the records that are created by them.

From the foregoing, all the different authorities and or sources reviewed are in agreement about the common threats to electronic data. They include: data corruption and loss, data theft, productivity loss, revenue loss, corporate humiliation, repudiation, damage, inappropriate content i.e. pornography, sabotage, espionage, cyber-terrorism, technological obsolescence among others. These threats may originate from within or without the organization. Regardless of their origin, viruses, Trojan Horses, and other malicious programs cause profound effects in monetary, psychological, and reputation terms to an organization of any size. There is therefore need for logical solutions to the several logical insecurities.

2.4 Physical threats

It will be an oversight to talk about logical threats to electronic facilities and data without saying a word on physical dangers. This ranges from natural disasters such as earth-quakes, floods etc to man-induced insecurity such as fire, malicious destruction and or vandalism among others. Man-made physical insecurity to electronic data and facilities is born out of shear malice by vandals or dissatisfied parties either from within or without the organization. For instance, in February 2003, vital computer records of the then Euro Bank that has since collapsed were destroyed to cover up suspect transactions. In a leading story appearing in the *Saturday Nation,* March 1, 2003, entitled "How Euro Debtors' files were destroyed; Computer smashed with hammer then debris burnt", a vivid account of how the destruction was done is given.

The following are excerpts from the report;

> Bank officials used a hammer to crush the hard disks used to store data in the computer's control system and then doused the debris with petrol and set it on fire, according to claims being investigated by fraud experts.....The Manager and Graphic Designer are suspected to have destroyed the computer components at a house in Westlands.....The destroyed hard disks contained the history of all the Bank's transactions, names of debtors and how much was owed by them to the Bank and beneficiaries of the fund.....The official said he had some computer records he wanted destroyed. He had brought along with him two computer servers, which were moved to a nearby Eldama Ravine Road and dismantled, removing the hard disks on which all the information was stored and crushed them with a hammer.....

The foregoing excerpts show that computer facilities and data are prone to dangers that may even be caused by those entrusted with the responsibility of safeguarding the same. In this case none other than the top Organization's Management and the Computer

System's Manager vandalized the Information Communication Ttechnologies and the information therein. Hence the need for physical security.

2.5 Measures

Electronic information and its related media face myriad problems or threats. Data security measures are intended to preserve and protect technology and information they transmit. The challenges of securing electronic information are many and complex. Securing technology and its data is no mean achievement as it is costly in terms of time and money.

Most of today's networks do not meet all security goals. The level of protection used depends on the value of security in a given application. Security measures are distributed throughout data communication networks. These measures can be implemented in host computers, terminals, modems, special security devices and transmission facilities. It is important to note here that whereas these are suggested remedies, they are however for reducing, rather than eradicating completely the said threats.

Mutonyi (2003:14) is of the view that a completely secure system is untenable. He asserts:

> No organization can claim that its network is completely secure. Any organization which may claim full proof security finds itself the target of hackers and crackers trying to prove that they can penetrate the security perimeters.

He goes further to point out the fact that a risk analysis needs to be undertaken to know the assets that need protection and the likely dangers facing them. He suggests that

organizations that deal with information would first need to do a risk analysis to determine what assets need to be protected and from what. He argues:

> Such organizations have to determine:
> - that a threat will disrupt information assets
> - Best way information assets can be secured
> - Sources from which information assets are to be protected.
> - From whom the information assets are being secured
> - The chance to protect information assets.

The security administrator of the organization, after identifying the security risks that the organization needs to safeguard itself from, has to develop a security policy. Such a policy must be issue driven and consistent with other organizational policies, acceptable by the network level staff and all levels of management. This will provide a way forward for establishing necessary measures to address issues related to data security.

System/logical security

Miller (2000.648) argues that security measures have to be as wide ranging as the nature of threats to electronic information resources. She adds that the measures have to be regularly updated to deal with the problem of obsolescence which is a major concern considering the present rapid technological change. Purser (1993.7) outlines the various security measures available against threats to electronic information. They include use of various forms of passwords, encryption or simply the backing up information in different formats and locations.

To the above, Sherman, K. (1998.302), adds access keys, organization and user ID, terminal ID, and operator authorization codes. He defines them as access items of a data processing system that are extensively used as identity from where the data is being accessed.

Passwords are the most common form of security. They are usually required by the computer, but can also be required by special security call back devices. These devices help to increase the security provided by the password. Remote users attempting to access a host computer using a modem must first enter their password and name into a call back device attached between the modems and the host. The device then checks the password for accuracy and, if the password is correct, hangs and calls the location programmed into the call back device necessitating uninterrupted communication.

Encryption is yet another important measure. Pursur (1993.7) defines encryption as the coding, or scrambling of data before it is transmitted over the communication link. The opposite of encryption is decryption, which refers to decoding, or the de-scrambling of the received data. It is one of the most thorough and effective ways to improve data security. Both encryption and decryption can be performed by host computers, front-end processors, or special encryption devices. A terminal can transmit plain or clear text to an encryption device, which encrypts or scrambles it, turning it into cipher text before sending it on. At the end of the communicating link, the cipher text is decrypted by a decryption device and sent on to the host computer as clear text or message as originally transmitted. The advantage of encryption is that those eavesdropping on the data transmission cannot understand the encrypted data. With encryption, public data networks over a satellite or microwave links can be used without fear of security breaches.

Confidentiality, as earlier mentioned, is one of the measures. This involves keeping confidential the content of users' data, traffic volumes, user identity and anything else, which is not to be generally known. To address the problem of information interception (eavesdropping), Onunga (1998:196) explains that Web browsers support some of encrypted communication. The most secure one is the secure society layer (SSL) protocol developed by Netscape communications...This protocol helps to ensure the authentication of both browser and the web server. It makes sure that everyone is who they are and helps to protect the privacy and security of communications.

Thus, authenticity ensures that, users' data and other information whose authenticity might be doubted are indeed genuine. Secure access management ensures that directly communicating parties such as a terminal and host computer or a host computer and PC are reciprocally convinced of the identities of each other. Proof of origin authenticates the originator and recipient of the data. Security control labeling are services that define and provide various levels of security and are particularly concerned with intervening between systems of different security characteristics. Data system integrity ensures that the sequences of data blocks or units received have not been altered and no units are repeated or missing.

To the above measures, Sherman (1998) adds,

> One other method of maintaining security, which may or may not be implemented on a data processing system, is the establishment and maintenance of a classification system, where physical access to the information is not permitted unless the potential accessor has

> appropriate physical authorization. In the case of documentation, this may be a specific clearance level identified by such items as a badge or special documents, while on a data processing system, this may be via the use of specific code words or use of specially pre-identified terminals.

Sherman is justified in arguing so since authorization is an indirect way of surveillance since it becomes easier to hold one responsible in case of any mess after accessing information Communication Technology facilities.

The Government of Kenya Information Communication Technology policy (2004:34) is in no conflict with Sherman's views in securing information. However, the policy divides information into "sensitive information control" and "sensitive information security". The policy articulates the following control measures for "sensitive information control":

(i) Information assets should be classified and protected according to their sensitivity and importance to the organization.

(ii) All sensitive information stored in any media should bear or be assigned an appropriate security classification.

(iii) All sensitive materials should be stamped and labeled accordingly.

(iv) Storage media i.e. floppy diskettes, magnetic tapes, removable hard disks, optical disks etc. containing sensitive information should be secured according to their classification.

(v) Electronic communications systems such as routers, switches, network devices and computers, used for transmission of sensitive information should

be equipped with suitable security software and if necessary with encryption or decryption software.

(vi) Procedures should be in place to ensure the secure disposal of sensitive information assets on all corrupted/damaged media or affected media both internal e.g. hard disk or optical disk and external e.g. diskette, disk drive, tapes etc to the systems.

On "sensitive information security", the policy isolates the following measures:

(i) Highly sensitive information should be classified.

(ii) Highly sensitive information assets should be stored on a secure removable media and should be in an encrypted format to avoid compromise by unauthorized persons

(iii) Sensitive information that is stored on fixed disks of a computer shared by more than one person must be protected by access control software such as passwords. Security packages must be installed which partition or provide authorization to segregated directories or files.

(iv) Removable electronic media must be removed from the computer and properly secured at the end of a work session.

(v) Removable electronic media containing sensitive information must be clearly labeled and secured.

(vi) Hard disks containing sensitive information must be securely erased prior to giving the computer system to another internal or external department or for maintenance.

To curb viruses, wide ranges of anti-virus software have been developed. They generally scan, identify and remove and or repulse known viruses. On the other hand Symantec client security suggest the use of outbound e-mail worm blockers which effectively stops the spread of worms via e-mail; Symantec recommends threat tracer application for quick identification of the source of attack, and for a fast targeted response.

According to the *"virus Bulletin Journal on Computer Virus and Anti Virus Products"* available at http: www.virusbtn.com/, the best way to secure a site or electronic information is by means of firewalls. Firewalls are like 'bouncers' stationed at strategic entry points to determine who should and who should not enter a given place. Firewalls check each packet that goes into a site, and decide whether to stop or let it go. Firewalls screen all access paths leading into network. The bulletin explains what a firewall is and how it works. That a firewall is an Internet packet (IP) filtering, which is the first level of security for packets entering a site or an organization's network. The 2nd level of firewall security is the modification of proxy services or server e.g. http, ftp, telnet etc to be security aware. This screens communications between computers.

However, Hey (1997.275) cautioned against underestimating the stamina and perversity of virus creators. Any such software should therefore be continuously updated to incorporate detection of viruses not yet created. It is usually advantageous to have a centralized server, effectively working as a hard disk for other workstations, where the anti-virus program is installed. Installation of self-deleting software can do the trick. This

is a kind of software that makes the virus delete itself as soon as it is introduced into the computer system.

To deal with the problem of obsolescence of hardware, recent research has been directed at creating a universal virtual computer with a common set of instructions that today's and tomorrow's computer can understand (The Daily Nation, June 2003). There is also need for a continuous update of both software and hardware to match the ever-changing technology. On the contrary, electronic records have to be migrated onto new systems in such a way that they can still be read and understood while maintaining their integrity and authenticity.

According to Thomas (1998:41), anti-spam measures are varied, from written protests to the advertisers, Internet Service Providers (ISPs) and relevant lawmakers to software that can detect and remove them. One can also filter spam out of their inbox, which, however, reduces the speed of the ISP's server.

Physical security

To protect information systems from physical insecurity such as the Euro Bank Computer Destruction, computer infrastructure, organizational standards, operating procedures and personal information have to be physically secured. Physical security involves placing the computers and related accessories in a controlled access, secure room or building. Access to all networking equipment must be controlled and information communication

technology room or centre be strictly out of bounds for unauthorized persons. This is as per Microsoft security advisor available at http://www.microsoft.com/security/defaul.asp.

According to the Government of Kenya Information and Communication Technology Policy Draft (2003:16), the following are suggested remedies to counter physical insecurity:

2.6 Site design

(i) The site should be located in a secure environment not prone to fire, chemical contamination or explosions.

(ii) Depending on the nature of operations, suitable floor structuring lighting, power and water damage protection should be provided.

(iii) Building construction should comply with safety regulations laid down by relevant government authority

(iv) Operational site should be constructed with fire resistant materials that are free from toxic chemicals.

(v) External walls should be constructed from brick or reinforced concrete of sufficient thickness to resist forcible attack. Ground level windows should be facilitated with sturdy grills or impact resistant laminated security glass. All internal walls must be from the floor to the ceiling and must be tamper resistant.

(vi) Air-conditioning system, power supply system and uninterrupted power supply units with proper backup should be installed depending on the nature

of operation. All ducting holes of the air conditioning system must be designed so as to prevent intrusion of any kind.

(viii) Organizations are encouraged to house their ICT facilities such as media library, electrical and mechanical control rooms in remote areas with access granted only to specific, authorized individuals on a need basis.

(ix) Any facility that supports mission critical and sensitive applications must be located and designed for reparability, relocation and reconfiguration. The ability to relocate, reconstitute and reconfigure these applications must be tested as part of business continuity.

2.7 Physical access

The draft policy further addresses the issue of physical access. It states,

(i) The responsibility for a 24 hour, seven days a week, three hundred and sixty days a year for the physical security of the protected systems and also actual layout at the site of operation should be defined and assigned to an authorized individual.

(ii) A biometric physical access security system should be installed at all high security installations to control and audit access to the operational site.

(iii) Physical access to the operational site at all times should be controlled and restricted to authorized personnel only. Personnel authorized for a limited access should not be allowed to gain access to the restricted areas within the operational site.

(iv) Dual control over the inventory and issue of access keys or cards during normal business hours at the data center should be in place. An up to date list of personnel in possession of keys or cards should be regularly maintained and archived for a period of three years.

(v) Loss of access cards/keys must be immediately reported to security supervisor of the operational site who should take appropriate measures to prevent unauthorized access.

(vi) All individuals other than operational staff should sign in and out of operational site and should be accompanied by operational staff.

(vii) Emergency exits should be tested periodically to ensure that the access security systems are operational.

(viii) All entrances to the data centers must be monitored round the clock by surveillance video cameras.

2.8 Fire protection

To cushion information technology facilities from fire, the government of Kenya in its ICT Policy Draft recommends the following:

(i) Combustible materials should not be stored within close proximity of the operational site.

(ii) Automatic fire detection system, fire suppression systems should be installed in compliance with the requirements specified by the ministry of public works at the operational site

(iii) Fire extinguishers should be installed at the operational site and their locations clearly marked.

(iv) Periodic testing, inspection and maintenance of fire equipment and fire suppression systems should be carried out.

(v) There should be no eating, drinking or smoking in the operational site.

(vi) Work areas should be kept clean at all times.

In a paper presented to the National Information and Communication Technology conference, the Ministry of Finance (March 2003:.6) recommends the following to enhance environmental protection of data systems.

(i) Water detectors should be installed under raised floors throughout the ICT sites and should be connected to audible alarms.

(ii) The temperature and humidity of the operation's site should be monitored and controlled periodically.

(iii) Information Communication Technology personnel should be trained to monitor and control the various fire and environmental protection equipment and other installed devices.

(iv) Periodic inspection, testing and maintenance of fire and environmental protection equipment and devices should be installed.

Sherman agrees with the above suggestion. He opines,

> another method of enhancing physical security is the implementation of a private communication facility. By so doing, a user will be able to protect more adequately the physical components over which information is being transmitted, whereas over a public communication network the same level of physical security

cannot be maintained.

Thus in conjunction with the private communications facilities, the user can also limit access to his entire physical facility, which will protect data, and as a second level of protection, limit access to computer room where the sensitive information is stored. These types of protection are used when data is considered to be in physical jeopardy (intruders, saboteurs, terrorists etc) or when otherwise authorized users have to be safeguarded physically from unauthorized users who share the same physical facilities.

Mutonyi (2003.150) classifies security measures into passive and proactive categories.

2.9 Passive measures

- Deterrent measures: since there is no known foolproof security, all necessary precaution must be employed to deter attackers.
- Responsibility measures: where the most trusted people are given the responsibility of being in charge of organization's overall security.
- Access should be given levels on a need to know basis thereby ensuring that people are only matched with the information they have been cleared to work with.

- Have strict passwords, user and organization ID policy and ensure that they match with the level of security of the organization.
- Firewalls should be installed at all choke points of the Organization

- Latest versions of firewalls should be installed and updated Regularly
- Data should be encrypted to ensure that only designated people will be able to decrypt information
- Procedures to authenticate all users of information should be put in place at all times.

To this, Steve West (2000:98), adds that Network security is all about safeguarding the operation and preserving the integrity in the face of accidental damage or deliberate attack. There are many aspects of security from privacy (ability to keep secrets) and integrity through to the 3As of Authentication (knowing who people are), Authority (allowing them to do only what they should) and Audit (the forensic trace, to see what happened, who did it and when and why).

2.10 Proactive measures

- Expect and anticipate the probability that the system can be broken into any time.
- Establish an elaborate procedure of monitoring the system intermittently so that all ongoing activities are logged to create a history of who logged or tried to log in and what information was being sought.
- Installation of trip wires to set off alarms as soon as an unauthorized activity is detected.
- Emergency response should be well defined and rehearsed periodically
- All known holes be perched

- After an attack, damage control should be attempted immediately.

International Records Management Trust (199928) is of the opinion that security officers have an important role to play to ensure that electronic data is protected from unwarranted access and destruction. It argues that by setting security standards and measuring compliance, they also help to ensure that sensitive information or confidential electronic data is protected. Security officers should carry out this role, in co-operation with the organization's management. They can achieve this through:

- Incorporating electronic data considerations into the policies, standards and practices governing the security and integrity of information systems.
- Conducting reviews of security of information systems in relation to electronic data.
- Advising data administrators on recent developments in the security field that could affect the management of electronic information
- Working with information managers and ICT managers to develop emergency plans that protect electronic Information
- Incorporating data management considerations into security awareness programmes.

It is evident from the above that security managers must set and maintain standards.

The identification of security services is thus not completely unambiguous and in any particular instance may require precise definition often in terms of the mechanisms, which provide the services.

The concept of security for electronic information is usually lagging behind in developing countries such as Kenya. As earlier mentioned, legislation to address this in Kenya was only tabled and enacted by Parliament in mid 2003 (Government of Kenya ICT Act, 2003). This was an Act of Parliament to provide for transactions carried out by the

means of electronic data interchange and other means of electronic communication commonly known as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information. It aims to legalize electronic delivery of services by the government, to protect privacy of individuals and interests of consumers of information technology services among other services. The reasons for the lag are related to lack and sometimes low level of training occasioned by inadequate funds and sheer information communication illiterate and or ignorant policy makers. Besides, it was not until the same period (2003) that our country formulated a semblance of national information policy, which deals with information, and data security among other issues. It is envisaged that this development will beef up war against real and potential dangers to information communication technology.

However, the current state of our legislation is dismally wanting as far as protection of our collective and individual interests relating to electronic domain are concerned. In support of this, Ngugi (2005.7), on law on cyber crime asserts that save for section 2 of the evidence Act which makes a comprehensive definition of the word 'computer' for purposes of the act, our entire body of statute law remains entirely oblivious of the pervasive changes and developments wrought by digital era. The problem however, is not one of prohibition, but enforcement. The nature of the World Wide Web and ever changing compounding complexity of electronic systems make the virtual arena difficult to administer accordingly complicating the investigation and prosecution of cyber crimes, a situation aggravated by the lack of, or weak statutory background to address these inadequacies.

Another inadequacy is lack of analogy between most cyber crimes and their conventional counterparts. For instance the penal sanction against trespass or breaking and entry cannot hold against an act of hacking into a computer network and unlawfully acquire proprietary data. Similarly, the act of perpetrating denial of service (D.OS) or damage to property cannot be prosecuted as such. This situation discloses the need for a comprehensive framework of legislation addressing specific threats to electronic activity and infrastructure. This is for the purpose of preempting the rise of cyber crime in its most nascent stages and to act in concert with the global community in combating cyber crime. Ngugi hastens to adda that apart from criminalizing certain acts, comprehensive legislation would bolster related spheres of legislation to make them relevant to the intricacies and challenges posed by electronic age law and order. Provisions of the criminal procedure code on preventive action by the police including search and entry need to be updated to accumulate the minutiae of investigating electronic crime.

Ngugi thus advocates for a complete overhaul of the law relating to security of electronic information to check the perpetration of cyber crimes, distribution of software used for illegal purposes, hosting of websites that provide resources for cyber criminals and dissemination of information that encourages the commission of cyber crime. Only such a legislative structure, one that captures emerging ethical notions that delineate minimum rights and liabilities of Internet users, can properly lay the juridical foundation for a predisposition to IT driven national development.

In a nutshell, the literature reviewed in this chapter attempts to establish ICT threats and measures to combat them. Since no research has hitherto been carried out on security of

ICT resources in Nairobi, the arguments advanced by the various authorities herein consulted identifies various threats and offers possible solutions to the threats in the research site. It is thus the research gap at the research area that this section has tried to bridge by way of relating the findings from elsewhere to our local situation.

CHAPTER THREE

Methodology

In this chapter, research methodology is discussed. These include; research design, population sample, sampling procedure and research instruments. These are the main procedures that were followed in conducting the study.

3.1 Reconnaissance

This study was conducted in various broad categories of public and private organizations, namely Financial, Information and Communication, Research and Academic. Initial familiarization visits were made to the focal organizations to introduce to the managers and staff the purpose of the study and review of proposed work and timetable. It was also at this stage that official permission was sought for research and interviewing both staff and users of electronic information. In institutions such as banks that were not willing to divulge security measures in place, information was gleaned from general literature.

The following were the key elements for conducting research

(i) Research design

(ii) Research site

(iii) Sources of data

(iv) Population sample

(v) Sampling procedure

(vi) Methods of data collection

(vii) Data collection instruments.

(vii) Data analysis and presentation

(viii) Data quality control

(x) Ethical issues

3.2 Research site

This study was conducted in Nairobi, which has a heterogeneous population and a big number of leading organizations. There is also a high concentration of ICT facilities and it is in Nairobi where they are heavily used. The area was also chosen because of its accessibility and resource limitations on the part of the researcher.

3.3 Research design

Initial visit was followed by pre-testing of the main questionnaire for staff and users in public organizations. This phase of the study was then followed by the main data collection. During this period, randomized visits were made to organizations where permission had been obtained to undertake the study. To begin with, one questionnaire tailored for staff and IT managers, was given to whoever that was in charge to fill at their own free time. Thirty respondents were targeted. This was followed up with an initial informal interview, along the lines of the study objectives that sought to fill in any gaps that may have been deemed useful. Two different questionnaires, designed for users and vendors, were also presented to every willing user visiting the organization's electronic resources and dealers (vendors) of the same resources. An effort was made to obtain at least ten users of an organization's facilities. Likewise, ten questionnaires were administered to ICT vendors. During the time spent in libraries and internet surfing, notes

were made regarding general usage of electronic information and their associated problems. Information gathered from the questionnaires, interviews, literature collection and general observations was then harmonized and directed towards achieving the objectives set out. Initial questions were aimed at assessing the capacity of the various institutions in terms of computers and associated facilities such as CD ROMS and back-up systems. Information on the computer literacy and or qualifications of staff deployed was sought from the heads of information services assessed.

The kind of rules and regulations in place were also sought for both from literature available and interviews with staff. User characteristics were also determined. Specific measures put in place to combat loss of these information sources were recorded. These included those that the users were not aware of e.g. monitoring e-mails and internet use. The level of computerization of each of the institutions was also assessed not just from the amount of hard and software but also its modernity.

Actual losses/damage including incidences of viral infections and tampering for the preceding year was recorded from records kept by the IT managers. Information on remedial measures in place where actual losses/damage took place was sought from literature on the organizations and from the managers. Also important was the information on the rate of replacement of hardware and software and acquisition of new electronic information.

In this case a descriptive survey was used for the study. It involved collecting data within a short period on a larger population with respect to one or more variables. The data was

collected on its natural setting hence not manipulatable. The interview and observation schedules ensured soliciting of detailed information to describe the situation as it was.

3.4 Sources of data

In this study, both primary and secondary sources of data were used. The following sources were consulted: ICT personnel, ICT users and ICT vendors. Secondary sources of data was basically review of documentary materials such as scholarly journals, theses and dissertations, Government documents, conference papers, books abstracts, periodicals, grey literature and the Internet sources.

3.5 Population sample

The population sample comprised selected public and private organizations in Nairobi using ICT in their operations. The organizations were basically Financial, Academic, Communication and Information oriented. Three groups of population samples were interviewed i.e. ICT Specialists, ICT users and ICT vendors. ICT specialists consisted of staff: mainly top management, middle management and ICT officers. The users were basically staff and other general users of ICT systems for the various needs. The final sample was ICT vendors. It comprised mainly of the management and sales representatives. The ICT specialists comprised a population of 30 respondents whereas the users and vendors consisted of 10 each all of whom were randomly selected.

3.6 Sampling procedure

The target population in this study was randomly selected from the entire Nairobi population to ensure representativeness. However, key informants were not randomly selected but interviewed on identification. The organizations' management that granted the researcher permission to undertake research did identification of key respondents. Such informants were mostly derived from the information technology sections.

3.7 Methods of data collection

The researcher undertook the research exercise personally. Four methods of data collection were used, these included: Questionnaires, interviews, observation and content analysis.

3.7.1 Questionnaires

A questionnaire is an instrument used to generate in any research activity. In the study questionnaires were synonymously used as instruments and a method of data collection. Questionnaires were both structured and unstructured. The unstructured questions were to avoid getting unnecessary data from the respondents whereas the structured questions aimed at getting more information that the researcher may have missed in close-ended questions. They thus gave the respondent enough space to make additional information of relevancy to the research objectives. The questions were printed and administered to three categories of respondents. These were information technology specialists, users and vendors of the same. A substantial number responded, some giving comprehensive variables whereas others only responding to closed ended questions. There were those

who kept on postponing the completion until they completely failed to respond. The questionnaires were geared towards gathering personal data, organization's bio data, kinds of information communications technology available in the organizations, their applications, threats that they face, security measures in place and how effective they are, competence of the staff and users in handling the technology and suggestions on how security could be enhanced in the organizations sampled for study.

3.7.2 Interviews

An interview is an oral administration of an interview schedule. This method was used since it gave room for a face-to-face transaction between the researcher and the respondents. It also provided in-depth data which was not possible to get using questionnaires, limited confusion because the researcher could clarify questions making the respondent to give relevant responses, was much more flexible than the questionnaires since the researcher could adapt to the situation and get as much information as possible and the researcher could clarify and elaborate the purpose of research and effectively convince the respondents about the importance of the research among other benefits.

Though this was envisaged as a method of doing the assessment, it was not satisfactorily used due to subjective response and lack of time on the part of respondents. They scheduled time for interviews but whenever the time for interviews was due, they cited pressure of work hence being too busy to grand interviews. This discouraged the researcher who now concentrated on use of questionnaires due to veiled resentment from

some targeted respondents. This method was only successful with users who freely shared their curiosity, interests, fears and frustrations with technology.

3.7.3 Observation on how ICT specialists and users interact with technology.

This was meant to gather first hand data on how ICT specialists and users interact with technology. It should however be pointed out that the researcher had no opportunity to enter the main data centers of the organizations studied as they are under restriction. Only institutional authorized IT personnel have access to the computer nerve centers. Though the researcher was disappointed that he was not given access to the data centers to see what happens, the experience taught him one fact, that restricting access and making the computer nerve centre out of bounds is in itself a measure of security to the technology and information it transmits. The researcher was able to freely observe the goings on in "branch" computer sections of the various departments of the organization studied, and was able to note the manipulation and manoeuver of technology by the specialists/staff and also users in their endeavor to search and disseminate information. This approach allowed the researcher to learn about some things, which otherwise had not been freely responded to through other research tools. Among the issues observed are:

- At the level of workstations and databases, some form of security either surveillance, passwords, user IDs or otherwise were in use.
- Various user groups required access security to particular information.
- Only a limited number of staff were involved in data processing for accountability purposes.

- Access to information was need-driven i.e. one needed to access the required information only without deviating to other files.
- Users and workgroups applied access control to information on a position, unit or staff basis. Thus the capability to view or edit information was restricted to authorized personnel only.

3.7.4 Review of documentary materials

This is basically content analysis. The researcher visited several information centres and libraries to consult existing documents to get an insight about the problem. The sources consulted cut across the entire body of knowledge. Primary, secondary and tertiary sources were reviewed and they gave the researcher a directional framework within which he operated. The researcher was able to know what had been done in this field by others elsewhere hence his decision to concentrate on organizations within Kenya in general but Nairobi in particular.

3.8 Data analysis and presentation

The data collected was summarized, manually coded and then keyed into the computer for analysis. Analysis was by use of the Statistical Package for the Social Sciences (SPSS). Where possible, presentations were made via simple tables, graphs and other statistical tools for comparisons.

3.9 Data quality control

Data quality control is a measure of data reliability; a degree to which a research instrument yields consistent results or data after repeated trials. Quality of a research study depends to a large extent on the accuracy of data collection procedures. Thus the instruments or tools used to collect the data must yield the type of data the researcher can use to accurately answer his or her questions.

In this study, the questionnaires, interview schedules and observation checklists were used by the researcher to yield reliable data; that is, data pertinent to the research goal, objectives and questions. In order to control the quality and reliability of the questionnaire as a research instrument, the researcher pre-tested the questionnaires to about 5% of selected samples, which were similar to the samples the researcher intended to use in the study. This enabled the researcher to rephrase his questions so as to convey same meanings to respondents to avoid different interpretations. Commends and suggestions made by the respondents during the pre-testing were used to improve the quality of questionnaires.

To yield quality and reliable data using interview technique, the researcher used neutral probing questions devoid of personal biases and subjectivity. The questions were thought of and jotted down before interview so as to have all the respondents subjected to the same questions.

As regards observation, an observation checklist was used to record what was observed during data collection. The researcher defined the behaviours to be observed and listed

them down. This helped the researcher to check off each of them as it occurs and in effect enhanced the accuracy of study.

3.10 Ethical issues

According to Mugenda, O (1999:120) Ethics is a branch of philosophy which deals with one's conduct and serves as a guide to one's behaviour. Against this background, the researcher maintained integrity throughout his research activities as he neither undertook the research for personal gain nor did the research hurt the interest of others whether personal or corporate. As a matter of ethics, all works referred to in this research have been acknowledged. The researcher treated the information given by respondents with confidentiality as promised in the request letter to the respondents to complete research questionnaires. As a matter of fact, respondents and organizations anonymity was kept especially those handling sensitive issues such as financial matters, which are supposed to remain as much confidential as possible. Only those organizations, which did not mind their actual names being used, were used.

In this study the researcher conformed to the principle of voluntary concept where the respondents willingly participated in the research this is because the researcher obtained their consent after disclosing reasons of undertaking the research and the intended use of research findings i.e. academic matters only. More so no vulnerable populations such as children, mentally disabled people etc were used in this research. Finally, in this research the researcher exercised academic freedom where unrestricted atmosphere for free

exchange of ideas and information was real. This is because the researcher was free to discuss and present findings without fear or favour.

3.11 Output

Notes that had been made during the period of data collection were incorporated into the general literature for report writing. A report was then compiled for submission to the Department of Library and Information Studies and Board of Postgraduate studies for assessment.

3.12 Limitations of the study

One major limitation of this study was the sample size. Four organizations, all located in Nairobi, may not adequately reflect the level of security threats to electronic information in all the different organizations in Nairobi. However the time available for the study (two months) and limited funding available precluded increasing the number of organizations to be sampled. Another limitation was that the study was focused on just organizations in Nairobi. This limits general application of the results to all organizations with digitized information in the country. However, it provides a good starting point for similar studies elsewhere.

CHAPTER FOUR

Presentation and analysis of data

The main purpose of this chapter is to discuss and present the results of data analysis in a systematic way. Data collected was coded and computerized. Data analysis then followed in line with the objectives presented. Some of the issues addressed along this line included general overviews in terms of ICT and electronic information in different categories of organizations, types of ICT facilities used, forms of security in place and recommendations for proper security of the facilities among other variables studied. Both descriptive and inferential statistics were used.

Descriptive statistics was used to describe a set or sets of data so as to yield meaningful information. They were used to derive condensed and summarized description of units in regard to enumerable or measurable characteristics. Inferential statistics were used to derive conclusions about a larger group or population from measurements of a smaller sample. Presentation was via tables, figures and commentaries (how and why) on variations in percentages and frequencies of response.

To begin with, data analysis and presentation was threefold. The first part is on ICT specialists and or staff in organizations studied. Part two is based on responses from ICT users whereas part three covers response from vendors. The variation in length and depth of the coverage is proportional to aspects studied in each category of organizations studied. The purpose of this part is to make presentations as per the data analyzed. It

presents results such as types and categories of organizations, ICT used in these organizations, threats to the ICTs and the possible solutions to the threats as shown by the respondents.

4.1 PART ONE: ICT SPECIALISTS AND OTHER STAFF

The main issues discussed are:

- Respondents' bio data
- Background information about the organization
- Specific electronic facilities in use
- Formal policy(ies) to regulate acquisition, use and maintenance of ICT
- Security measures in place to safeguard the facilities
- Physical media Security
- Disaster preparedness and recovery plan
- Costing or charging of services offered
- Other problems associated with electronic information
- Suggestions and recommendations

4.2 Age of respondents

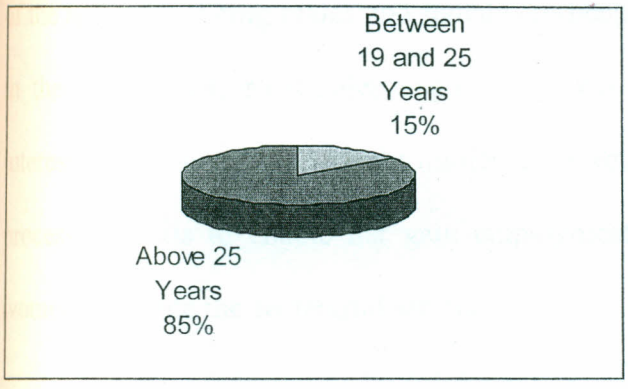

Fig. 1: Age of respondents.

The researcher wanted to establish the age bracket of people specialized in ICT. It was established that the majority of the IT specialists i.e. 85%, are above 25 years of age with only 15% being between 19 and 25 years. This is because in Kenya most people get employed from the age of 25 years, when they are through with professional training. Further, people of the ages less than 25 years could still be learning to become IT specialists.

4.3 Gender of respondents

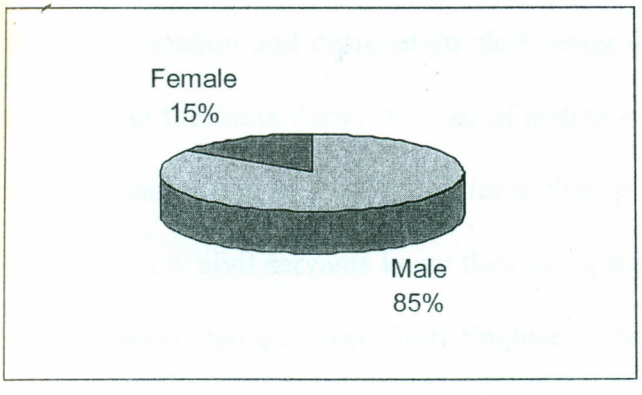

Fig. 2: Gender of responents

In most of the organizations in Kenya, males dominate the IT industry with 85% and 15% of the specialists being males and females respectively. This is due to the fact that until in the recent past, electronics engineering was a man's dominion whereas female's interests in computers were only limited to secretarial sphere. Once one acquired word processing skills to enable her gain employment, she was satisfied. Indeed, to date, women dominate the secretarial service.

4.4 Occupation of respondents.

	Frequency	Percent
Engineer	1	5.9
Archivist	2	11.8
IT Technician	3	17.6
Programmer	2	11.8
Accountant	1	5.9
Telecommunications Technician	2	11.8
Lecturer	3	17.5
Computer Operator	1	5.9
Civil Servant	2	11.8
Total	17	100

Table 1: Occupation of respondents.

Despite occupation and designation slots being distinct, most respondents confused the two to mean the same thing. Instead of stating one's occupation most respondents gave their designation and or responsibilities at their place of work. Of the population studied, only 11.8% i.e. civil servants knew their occupation. Table 1 shows the designations of the population-studied range from Engineers, Archivists, IT technicians, Programmers, Accountants, Lecturers, Telecommunication technicians to Computer operators

4.5 Category of organization

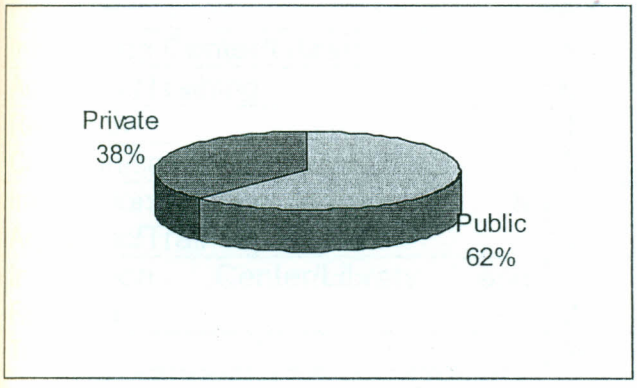

Fig. 3: Category of organizations

The researcher sought to know the name and category of organizations. The organizations were categorized as public or private. It emerged that 62% of the organizations studied were public while 38% were private. The sharp difference was occasioned by the fact that public organizations were more willing and accommodating to researchers than private organizations which are closed for fear of business competitors 'breaking into their secrets of business success'. Government institutions have embraced more and more ICT applications in their daily operations. This may also be the case with private organizations though the percentage studied is less than that of public organizations.

4.6 Type of organization

	Frequency	Percent
Financial	5	20.8
Information Center/Library	4	16.7
Academic/Training	6	25
Research	1	4.2
Communication Institution	5	20.8
Information Center/Library & Academic/Training	1	4.2
Information Center/Library and Research	2	8.3
Total	24	100

Table 2: Type of organization

For reasons of confidentiality and privacy, organizations studied could not be given their actual names. They were camouflaged under the tag 'type' of organization as shown above. For instance, the financial institutions studied were able to positively give response without fear of being logically invaded by cyber crooks. Other types studied included information centers/ libraries, academic cum training, Research and Communication organizations. From table 2 above, Academic cum training organizations yielded the highest response rate (25%) followed by Financial and Communication organizations at 20.8% respectively. This is because of the high rate of users in academic organizations, hence hiring of more staff to manage ICT and its related information. This also applies to financial and Communication organizations. Information Centers and or libraries recorded 16.7% whereas organizations serving as Academic cum training registered 4.2%. The total percentage of organizations studied stood at 100 whereas the total frequency was 24.

4.7 Year of organization establishment

Year	Frequency	Percent
1948	1	5
1953	1	5
1960	4	20
1963	2	10
1965	3	15
1966	1	5
1969	3	15
1972	1	5
1992	3	15
1999	1	5
Total	20	100

Table 3: Year of organization establishment

Most organizations were established as early as 1948 and as late as 1999. They have been in existence in the country for over 50 years and have stood the test of time.

4.8 Purpose and functions of organizations

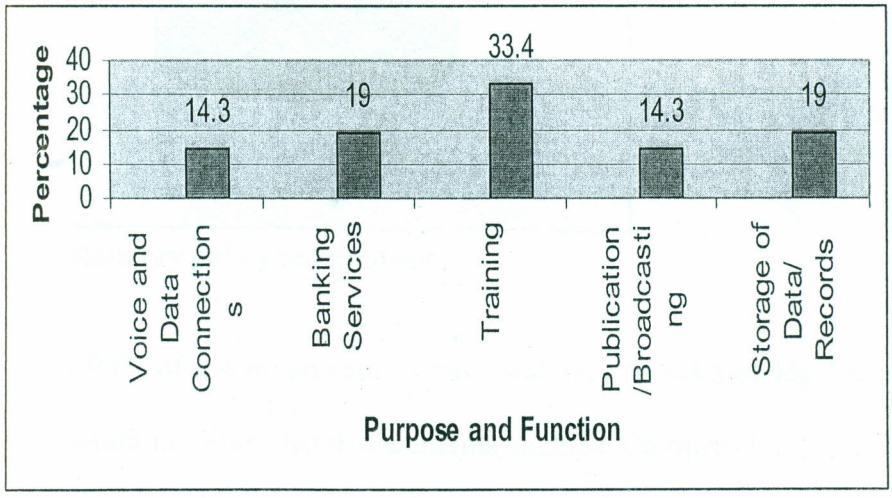

Fig. 4: Purpose and functions of organizations

The functions are organization dependent. The organizations are communications organizations, Financial, Academic and Training organizations. Others were broadcasting organizations and Information centers. Among the functions clearly shown for the various organizations are voice and data connections, banking services, training, publication/broadcasting, storage of data and records among others that are not reflected in the table above. The figure above shows that training is the leading function of organizations at 33.4% followed by banking services and data storage and records management at 19%. Voice and data connections as a function, together with publication/broadcasting recorded 14.3%. Other functions and purposes of the organizations include banking services and the media, both print and electronic.

4.9 Statutory policy requirement

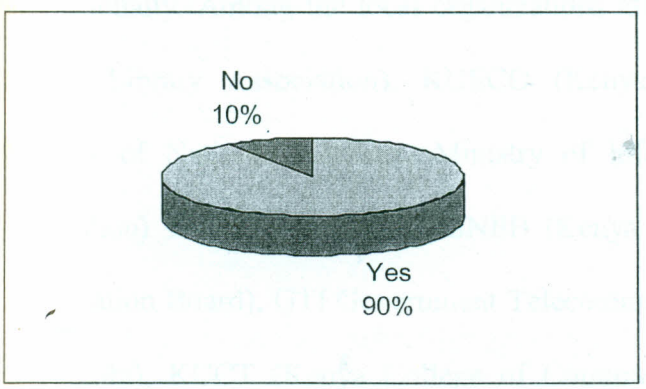

Fig. 5: Statutory policy requirement

At least 90% of the organizations have statutory policies or legal provisions that guides their operations. Such legal documents include Co-operatives Act, University Charter, Communications Act, Software Amendment Act-1998, Audit Bureau of Circulations, Public Archives and Documentation Service Act and E-Government and E-Security Act. Only 10% of the respondents appeared not know of the existence of such policies.

4.10 Affiliation/attachment to local or international Organizations

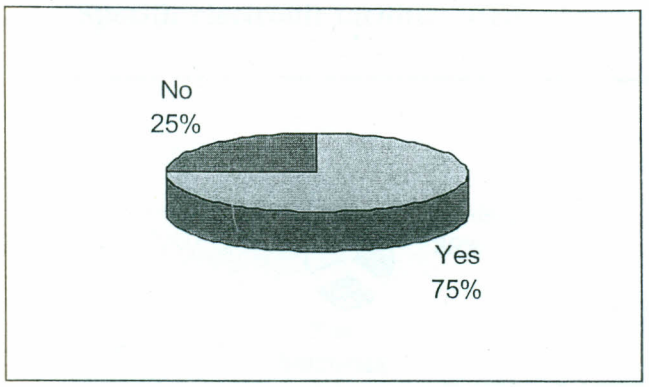

Table. 4 Affiliation to Local/International organizations

Most of the organizations do not operate independently. They are interdependent for support purposes. About 75% of them are affiliated to other organizations locally and internationally. Among the local organizations affiliated to those under study are: KLA (Kenya Library Association), KUSCO (Kenya Union of Co-operative Societies), Ministry of National Heritage, Ministry of Information, KBC (Kenya Broadcasting corporation) Telekom Kenya, KASNEB (Kenya Accountants and Secretarial National Examination Board), GTI Government Telecommunication Industries), UON (University of Nairobi), KCCT (Kenya College of Communication Technology), JKUAT (Jomo Kenyatta University of Agriculture and Technology), KIPS (Kenya Information Preservation Society), Safaricom. International organizations affiliated to these organizations are AIU (Alliant International University), ICA (International Council on Archives, Monitor Daily, KLA (Kenya Library Association), IFLA (International Federation of Library Associations), COMLA (Commonwealth Library Association), SCECSAL (Standing Conference of East, Central and Southern Africa Librarians),

Reuters, URTNA, AP (Associated Press) and British Telecom. Only 25% are not affiliated to other organizations.

4.11 Specific electronic facilities used

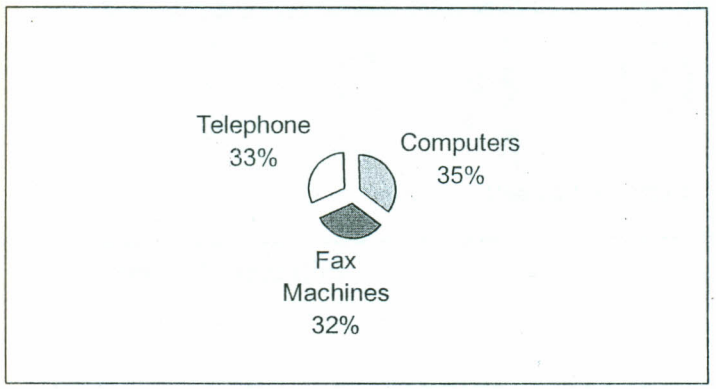

Fig. 7:specific electronic facilities

The figure above shows that electronic facilities are used at organizational level. Of all the facilities available in the organizations, computers were highly used. Computer usage stands at 35%, while telephone facilities at 33% and 32% for fax machines and other facilities respectively.

These facilities are used for different purposes such as general office work, data computation, archiving, updating client's data, E-mailing and E-commerce such as quotations and tendering processes and training. See figure 8 below.

4.12 Uses of IT facilities.

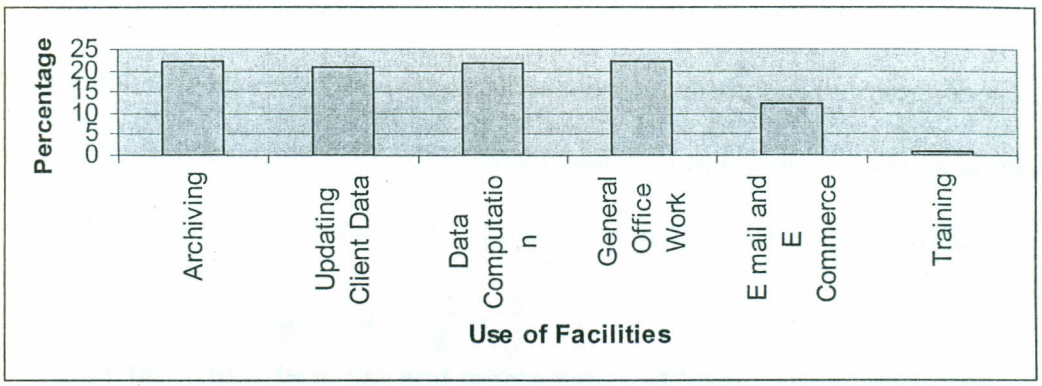

Fig. 8: Uses of IT facilities

Figure 8 shows the various uses made of ICT facilities. About 80% of the facilities are used for archiving, updating clients' data, data computation and general office work, each accounting for about 22%. It seems like these are the core objectives of the organizational ICT facilities. The rest of the uses of the facilities are E-services such as e-mails and e-commerce, which were cited by about 11%; training usage accounted for about 1%.

4.13 Use of telephone/ fax facilities

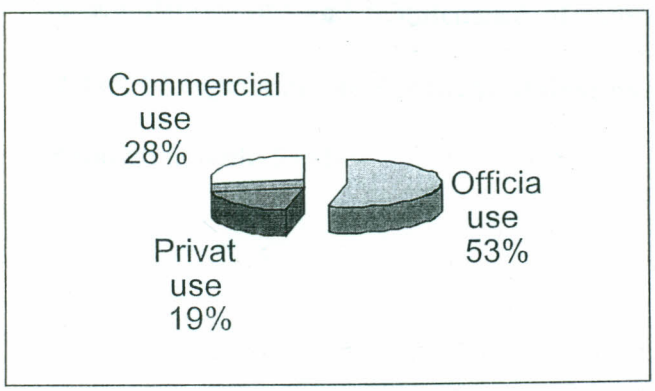

Fig. 9: Use of telephone/fax facilities

It is worth noting that the electronic facilities use cuts across private and official reasons. They are also used for commercial cause. Of the telephone and fax facilities used, 53% are used for official purposes, 28% for commercial use and 19% for private use. It emerges that official use is the highest since most organizations put premiums on official usage only. However, in some other organizations, limited private use is allowed. The organizations also allows commercial exploitation of their electronic facilities.

4.14 Policy for acquisition, use and maintenance of information/ equipment

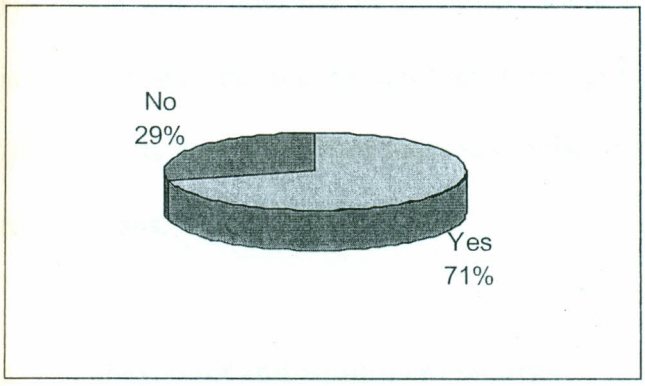

Fig. 11: Acquisition, use and maintenance of information/equipment.

In 71% of the IT specialized organizations; there are formal and or informal policies that regulate acquisition, use and maintenance of information and equipment. The policies were developed depending on objectives of their mother organizations between 1972 and 2002 as shown in table 5 below.

4.15 Year of policy development.

Year	Frequency	Percent
1972	1	10
1978	1	10
1996	2	20
1998	1	10
2000	1	10
2001	1	10
2002	3	30
Total	10	100.0

Table 5: Year of policy development

From table 5, it follows that of the organizations studied, only two had policies developed in the 1970s whereas the rest developed their policies in the late 1990s and from the year 2000. This is due to the fact that most policies were developed at the inception of the organizations.

4.16 Policy, data and equipment security.

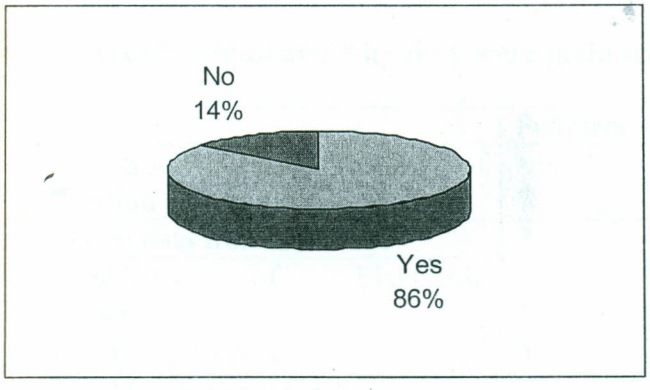

Fig. 11: Policy, data and equipment security

Of the policies developed by the IT specialists 86% had captured the element of data and equipment security and only 14% had not captured this element.

4.17 Why policies were developed.

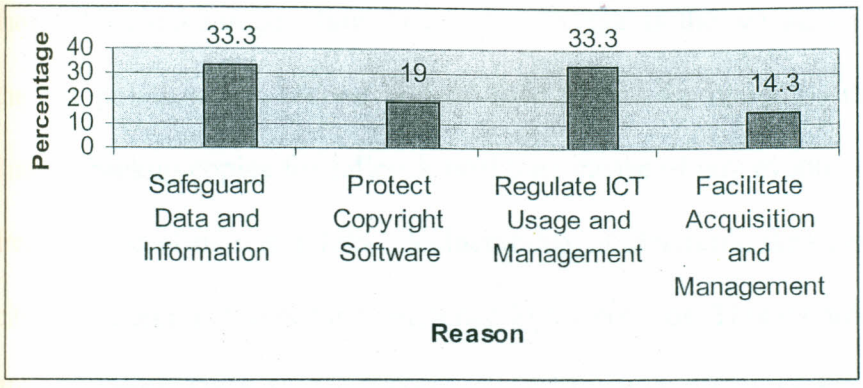

Fig. 12: Why policies were developed.

From figure 12, majority of organizations developed ICT policies to safeguard data and information and regulate ICT usage and management. This accounts for 33.3% of the responses. Protection of copyright software was another reason cited for policy development. This was cited by 19% of the respondents in organizations studied. Others attributed policy development to the purpose of facilitating the acquisition and management of the ICTs.

4.18 Security elements: why they were included in the policy

	Frequency	Percent
Protect Sources and Privacy of Information	7	35
Safeguard data from Sabotage	7	35
Vulnerability of Electronic Equipment	2	10
Make Backup Copies	3	15
Reduce Maintenance Costs	1	5

Table 6: Why security elements were included in the policy

Table 6 shows that security elements were included in most of the ICT policies. They comprise: protection of sources and privacy or confidentiality of information, which

registered a frequency of 7 and 35% response. These figures were equally registered for those who cited safeguarding data from sabotage as the reason for including security in the ICT policies. The second highest cited reason for including the security element is making backup copies for fallback positions incase of any eventuality. This stood at the frequency level of 3 and 15%. Vulnerability of electronic data and equipment was also cited as an element of security included in the policies. This recorded 2 as frequency and 10% response. Only 5% at a frequency of 1, cited reduction of maintenance costs for inclusion of the security element in the policies.

4.19 Security aspects covered in the policies

	Frequency	Percent
Antivirus	3	10
Security Guards	2	6.6
Copyright Protection	4	13.3
Copyright Law	2	6.7
Use of Passwords	5	16.7
Data Integrity and Security	5	16.7
Firewalls	2	6.7
Restriction of Unauthorized Users	4	13.3
Encryption	3	10

Table 7: security aspects covered in the policy

The major components of the security aspects covered in the policies developed are the use of passwords, data integrity accounting for 16.7% and a frequency of 5 each, copyright protection and restriction of unauthorized usage accounting for 13.3% and a frequency of 4 each. Antivirus protection and encryption accounts for 10% and a frequency of 3 for the aspects of security covered. Copyright law and firewalls are

covered in 6.7% at a frequency level of 2, while security guards are accounted for at a frequency of 2 and 6.6. % of the policies formulated by these organizations.

4.20 Measures against internal threats

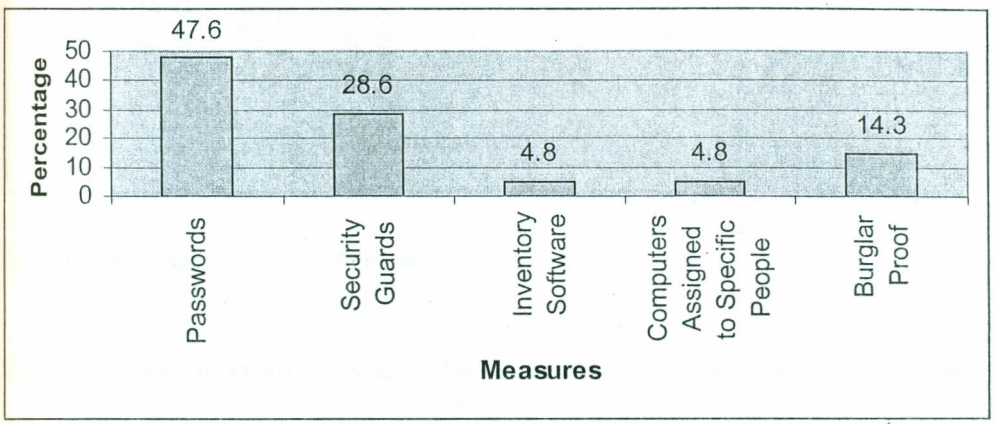

Fig. 13: measures against internal threats

The above illustration shows that measures against internal threats are both logical and physical. For logical measures, 47.6% of the respondents showed that passwords are used while 4.8% suggested use of anti virus software and another 4.8 % suggested that computers should be assigned to specific people. This serves to achieve both systems and physical security. To guard against internal physical threats such as the physical crushing of the computer servers by the management and IT staff, 14.3 % of the organizations employ the use of burglarproof facilities.

4.21 Measures against external threats

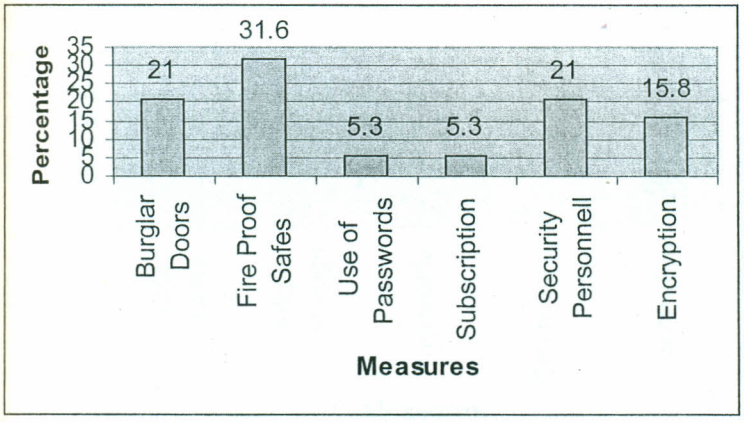

Fig. 14: Measures against external threats

Since information communication facilities face external threats, the organizations under study use the following measures in order of their rankings: Fireproof safes 31.56%, burglarproof doors and security personnel 21% respectively. These are measures to combat physical external threats. To address logical external threats, passwords and subscription were suggested by 5.3% each. Encryption was cited by 15.8% of the sampled population.

4.22 Measures to ensure confidentiality of ICT by products

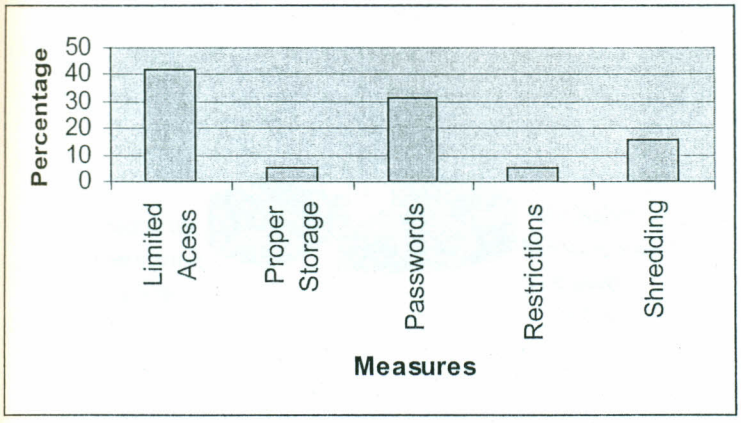

Fig. 15: Measures to ensure confidentiality of ICT by- products

Limiting access to facilities was the most commonly used method of ensuring by products' confidentiality. Other methods used are passwords, proper storage, shredding and restriction in the use of the facilities. Limited access is the popular most measure cited by about 42% of the respondents, followed by use of passwords, which was supported by 32% response. The other measures comprise shredding at 17% response, restrictions and proper storage, which was endorsed by 0.5% each.

4.23 Measures against masqueraders

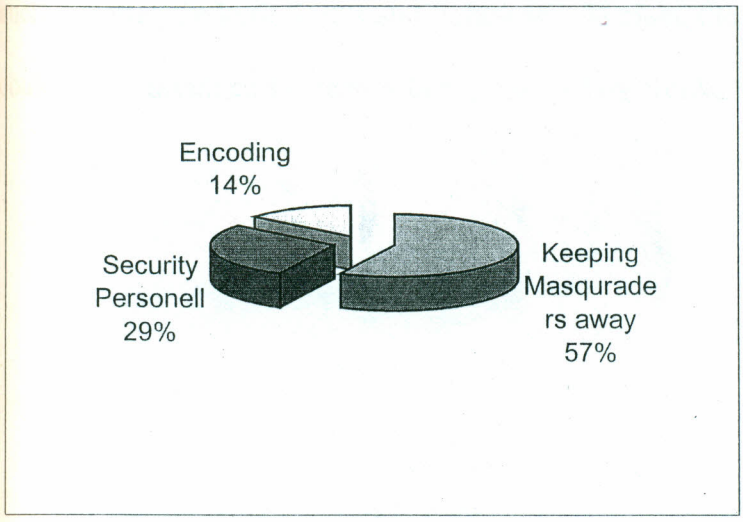

Fig. 16: Measures against masqueraders

Though not shown how, keeping masqueraders away was suggested as a measure by 57% of the IT specialists. Those who used encoding to check against masqueration were 14% while those who exploited services of security personnel were 29% respectively.

4.24 Measures against interception

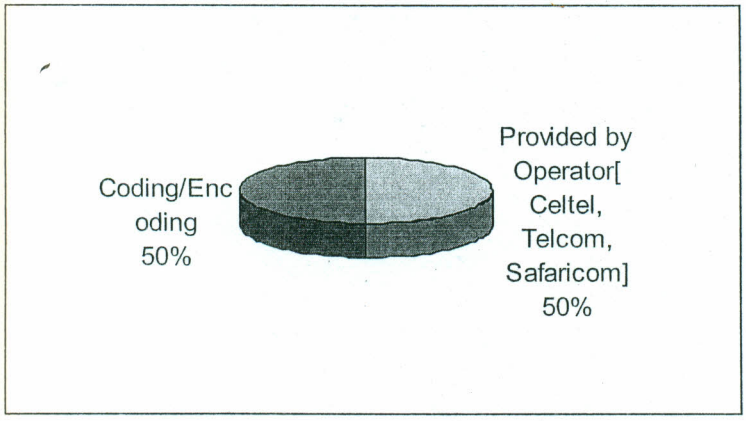

Fig. 17: Measures against interception

The only measures used against interception were those provided by service providers such as Celtel, Telkom Kenya and Safaricom. At most, the measures are confidential and could not be divulged for fear of being misused by crooks to make their work difficult.

4.25 Measures against dubbing

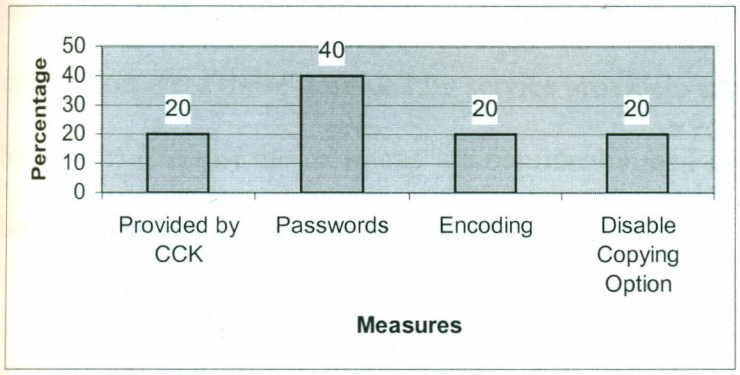

Fig. 18: Measures against dubbing

The use of passwords against dubbing was the highest precaution in most of the organizations. Disabling of the copying option, encoding and services provided by Communication Commission of Kenya was depended on by 20% each of the IT specialists.

4.26 Transmission security measures

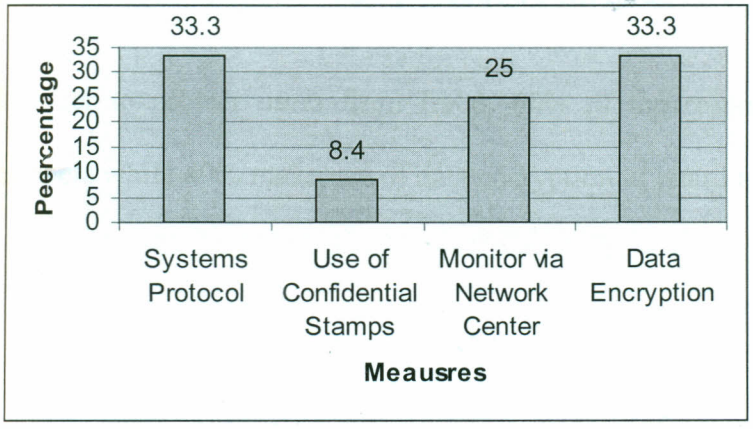

Fig. 19: Transmission security measures

Control and securing of data transmission is through data encryption and systems protocol, which were cited by 33.3% of the respondents. Monitoring via network centre

and use of confidential stamps are used as security measures by 25% s and 8.4% of the specialists respectively all-adding up to 33.8%. The only measures used against interception were those provided by service providers such as Celtel, Telkom Kenya and Safaricom. At most the measures are confidential and could not be divulged for fear of being misused by crooks to make their work difficult.

4.27 ATMs and credit card protection from fraud

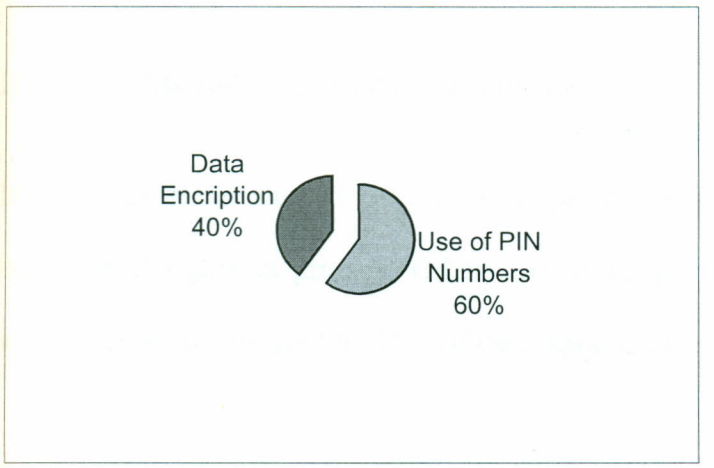

Fig. 20: ATMs and credit card protection from fraud

In order to protect users from fraud, 60% of the respondents suggested use of PIN numbers while 40% make use of data encryption to guard against fraud.

4.28 ATMs and credit card users' privacy

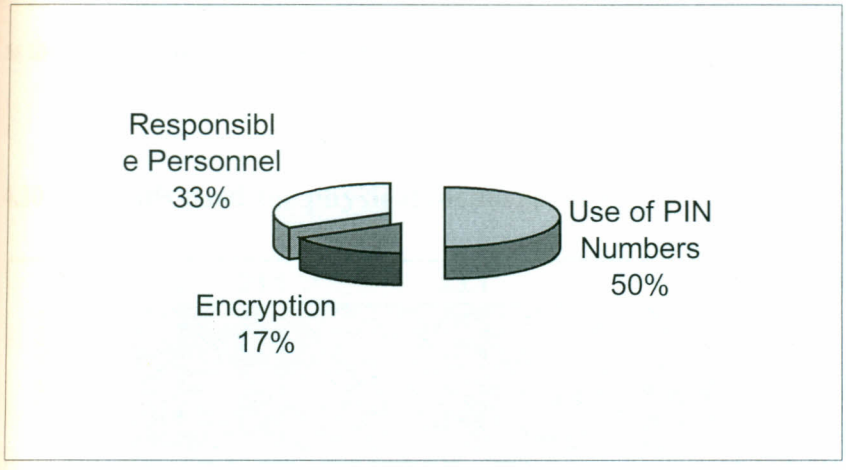

Fig. 21: ATMs and credit card users' privacy

In the organizations studied, 50% of the population makes use of PIN numbers to protect their clients' rights to privacy. Others (33%) assign facilities to responsible personnel while encryption was used by 17% of the respondents.

Use of PIN numbers was the only measure used against ATMs and credit card protection from unauthorized access.

4.29 Electronic money transfer security

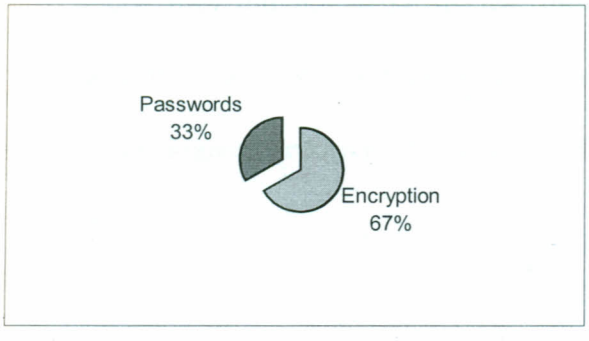

Fig. 22: Electronic money transfer security

Security Measures used in electronic money transfer are encryption and use of passwords accounting for 67% and 33% respectively. Since encryption is complex, it is highly rated as the best option to secure data.

4.30 Methods used for physical media security

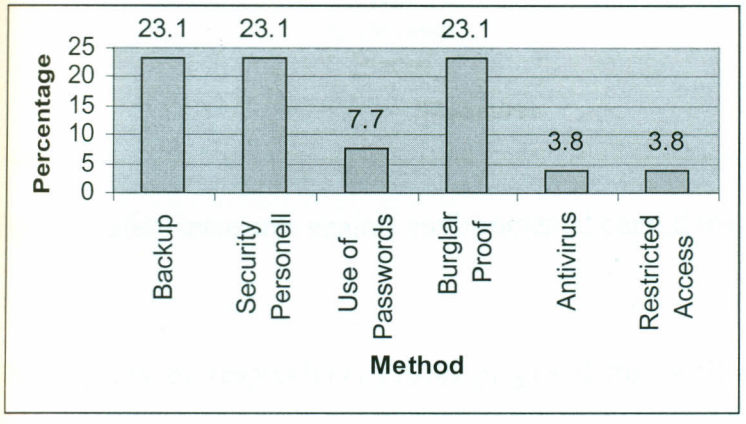

Fig. 23: Methods used for physical media security

In Fig. 23, respondents suggested various methods to ensure physical media security. Those highly employed are information backups, use of security personnel and burglarproof installations all of which accounted for 23.1% each and a total of 69.3%. Though use of passwords and ant virus-measures were suggested by 7.7% and 3.8% respectively, they did not make it clear how these measures could guarantee physical media security since conventional wisdom has it that they are best used in safeguarding system's or logical security. A further 3.8% suggested restricted access as a good measure.

4.31. Safety measures against environmental conditions

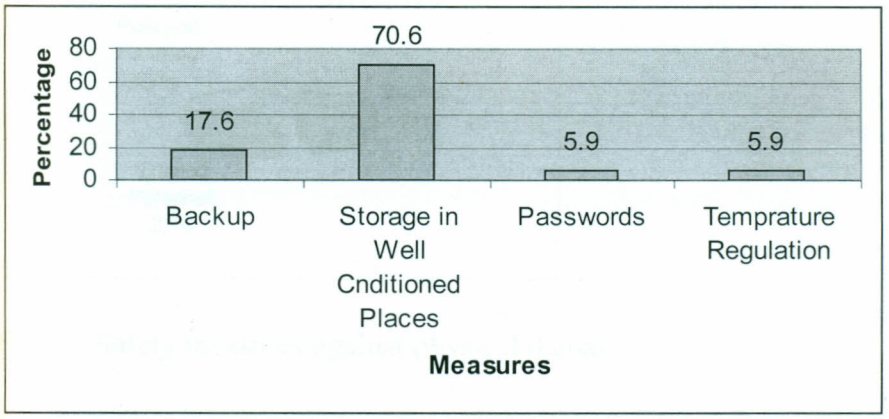

Fig. 24: Safety measures against environmental conditions

The majority of respondents (70%) proposed that well conditioned storage places are ideal for regulating or checking against adverse environmental conditions. Others (17.6%), recommended the use of back ups so that in case of any negative effect; an organization can have an alternative to fall back to. Again, 5.9% of the respondents mentioned use of passwords, which is a misplaced measure. It is unfortunate that such a misunderstanding comes from IT specialists. The reason for such deviance is perhaps lack of understanding on how passwords are used. Temperature and humidity regulation was cited by 5.9% of the respondents. It is unfortunate that such a misplaced response comes from ICT specialist.

4.32 Safety measures against physical damage

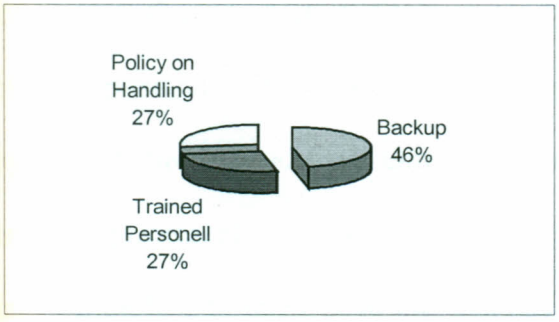

Fig. 25: Safety measures against physical damage

Backing up of information resources is yet again a dominant measure of securing from physical damage. Back up of information was supported by 46% of the respondents. Of the remaining 54%, 27% suggested development of a policy on handling information resources while another 27% advocated for the use of trained personnel as security measures.

4.33 Safety measures against technological obsolescence

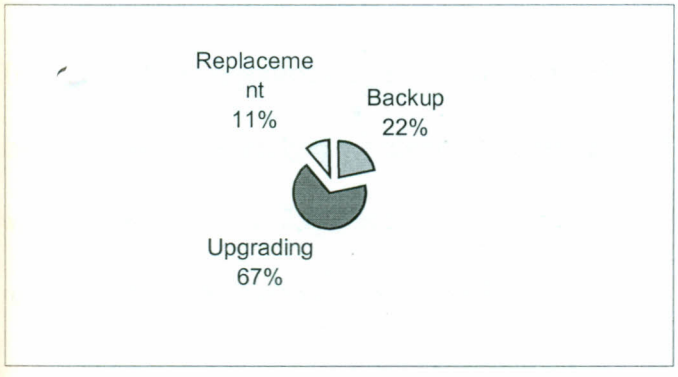

Fig. 26: Safety measures against technological obsolescence

As a problem, technological obsolescence can be countered by upgrading of the Information Communication Technology systems. This suggestion was backed by 67% of the respondents. Back up of information through emulation and migration was raised by 22% of the respondents. Only 11% suggested replacement of the systems by new ones. Replacement received minimum suggestion since this may result into permanent information loss through or in the obsolete equipment, hence backing up and upgrading being the best measures.

4.34 Safety measures against vandalism

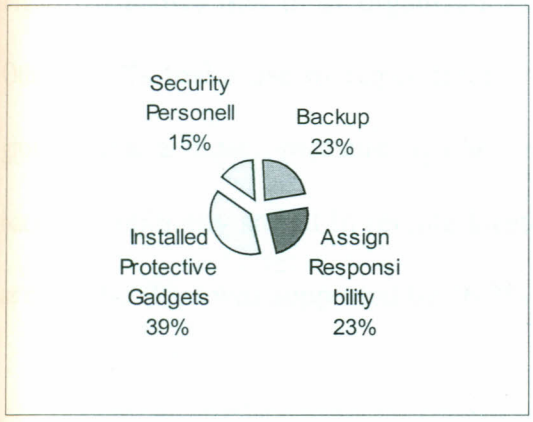

Fig. 27: Safety measures against vandalism

To protect ICT resources from vandalism, 33% of the respondents suggested use of installed protective gadgets, backups and assignment of responsibilities to specific people was pointed out by 23% each by the respondents. Only 15% of the respondents suggested the use of security personnel.

4.35 Measures against floods

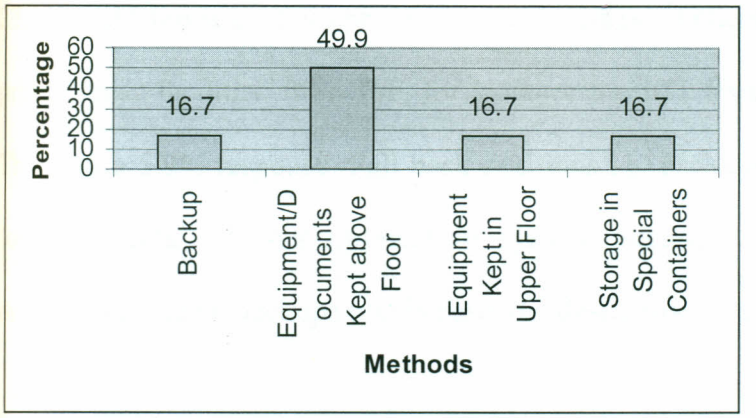

Fig. 28: Measures against floods

Figure 28 shows that most organizations (49.9%) store their facilities above the floor. Other 16.7% make use of upper floors for the same purposes. This is because raised grounds are a safety measure against foods. The other measures employed include backups preferably stored in remote locations and use of special storage containers such as cabinets. This was supported by 16.7% each of the sampled populations.

4.36 Measures against fire

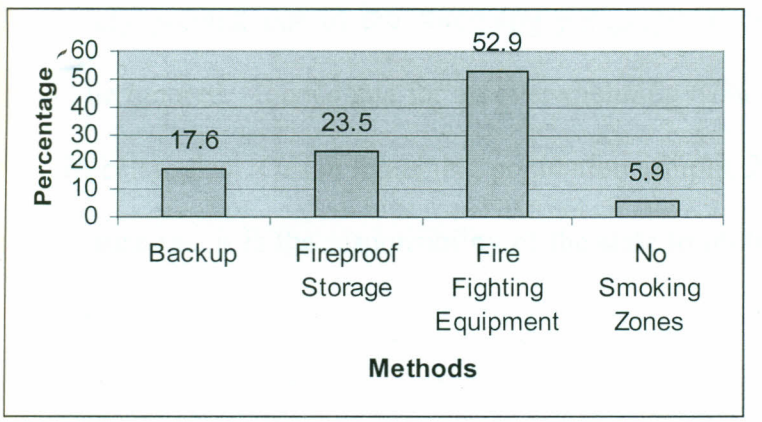

Fig. 29: Measures against fire

In case of fire menace, 52.9% of the organizations use fire-fighting equipment while 23.5% add the use of fireproof storage facilities. Others take preventive measures to protect their facilities from fire, for instance the ICT areas are a "No smoking zones." This was a 5.9% response. Fall back positions i.e. backups seem to cut across solutions for all threats, whether physical or systems security. In this case, 17.6% of the organizations have backups just in case of a destructive fire catastrophe.

4.37 Measures against wars and terrorism

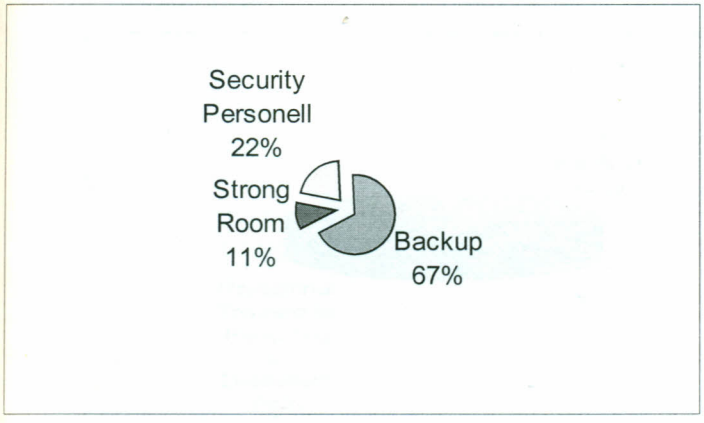

Fig. 30: Measures against wars and terrorism

As already pointed out in the foregoing paragraph, backup as a measure of security cannot be ignored. It accounts for an overwhelming 67% as a measure against wars and terrorist calamities. Of the remaining population sample, 22% gave security personnel as the measure i.e., it is the responsibility of the state to protect its boarders from wars and terrorism.

4.38 Measures against other perils

The only measure used against other perils is backup. It is thus clear that backing up of Information is an integral security measure which features in all forms of ICT security. If an organization has to ensure maximum protection of its ICT facilities, and or information, it is better advised to store them in different remote areas to safe itself from a rainy day.

4.39 Disaster preparedness, management and recovery plan

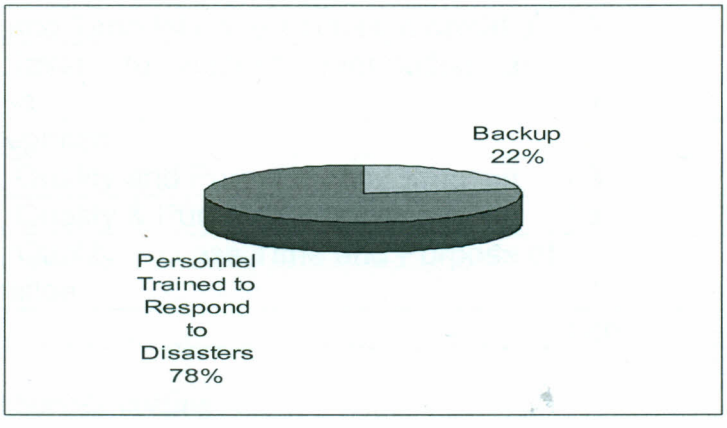

Fig. 31: Disaster preparedness, management and recovery plan

For organizations that acknowledged having disaster preparedness and a recovery plans, 78% undertake regular training of their personnel in readiness for disaster management. In addition, others suggest remote back ups as an alternative in case disaster befalls the organization. This accounts for 22%.

Most organizations cost their services. There are different aspects taken into consideration while costing services offered by the organizations. They include quality of information, time taken to access information, and the purpose for which the information

is going to be used e.g. If information is sought for commercial reasons, then one is likely to pay more than one who seeks information basically for research purpose. In a tabular format, the aspects considered for costing services are thus:

4.40 Costing of services offered

	Frequency	Percent
Value	1	3.8
Quality of Information	1	3.8
Time taken to Access Information	5	19.2
Purpose	2	7.7
Value and Quality of Information	1	3.8
Value and Time taken to Access information	1	3.8
Time taken to Access information and Purpose	1	3.8
No Response	7	26.9
Value, Quality and Purpose of Information	3	11.5
Value, Quality & Purpose of Information	3	11.5
Value, Quality, Access Time and Purpose of Information	1	3.8
Total	26	100

Table 8: Service costing

The table above indicates that 26% of the respondents did not respond on the question about service costing. This is perhaps due to lack of information about services charged and the criterion used to cost them. About 19.2% charge according to time taken in making use of the facilities while 11.5% charge according to value, quality and purpose of information. However most of the organizations' service costing is dependent on quality of information, value of information, time taken to access information and purpose of information all of which accounts for 3.8% response.

4.41 Ranking of security measures

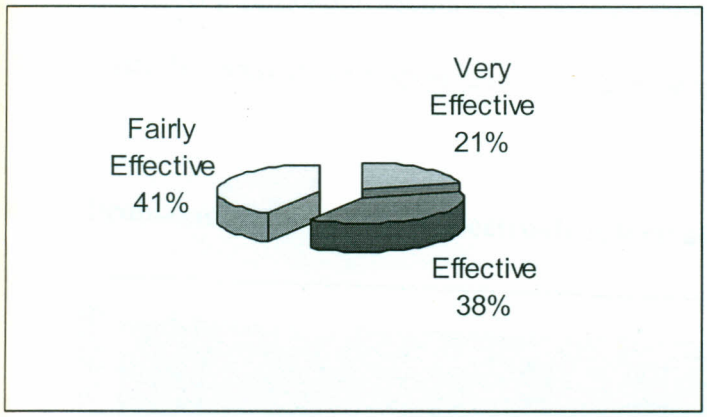

Fig. 32: Ranking of security measures

Since the organizations studied had ICT facilities then it followed that there was a way of preserving or safeguarding them from harm. The researcher wanted to know how effective the security measures in place were. It emerged that 41% of the respondents said that the security measures used are fairly effective. Other respondents (38%) rated the security measures as being effective. Only 21% of the respondents rated security measures in their organization as being very effective. Thus the measures used were on the average effective. However, in a turbulent cyber world where marauding cyber crooks are the order of the day, much more than just average measures need to be put in place.

4.42 Other Perils

Apart from the realization by the researcher that electronic information and its related infrastructure is prone to many dangers which may be physical or logical in nature, he wanted to establish from the respondents if there are other problems bedeviling information communication technology, besides those known to him. The figure below shows what the majority of respondents cited as inherent threats to ICT.

4.43 Problems associated with electronic information

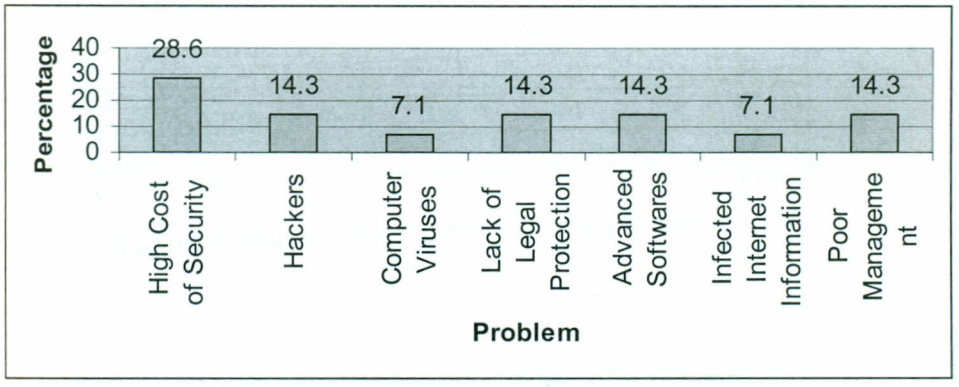

Fig. 33: Problems associated with electronic information

NB. The noun 'Problems' as used in this variable is synonymous with threats or insecurity facing electronic information and its infrastructure. The main problem associated with electronic information in some organizations is the high cost of security. In 20% of the organizations studied, high cost of security was cited as an impediment. This is in regard to installation and maintenance of full proof security systems. The other problems or threats cited by 14.3% of the respondents include hacking, lack of legal protection and poor management structure of the ICT equipment. Though some respondents mention advanced software as being problem, it is not clearly elucidated, if anything, it should have been cited as a measure rather than a problem. Other problems

pointed out by 7.1% of the respondents are computer viruses and infected Internet information. Thus electronic information and its related infrastructure are faced with myriad problems or dangers that are in dire need of solutions.

4.44 Recommendations to address security problems

Recommendation	Frequency	Percent
Reduce Cost of IT Equipment	2	7.7
Online Processing by User Departments	1	3.8
Better trained personnel	2	7.7
Upgrade antivirus	1	3.8
Limit Internet Access	2	7.7
Policy on preservation of Electronic Records	2	7.7
Discourage Foreign Diskettes	1	3.8
Burglar Proof Buildings	1	3.8
No Response	14	53.8
Total	26	100.0

Table 9: Recommendations to address security problems

Table 9 shows some suggested solutions to some of the ICT threats cited in fig. 15 above. It should however be clear that neither all the respondents gave recommendations nor are the recommendations given exhaustive. About 53.8% did not complete the section on recommendations may be due to lack of what to suggest or some other reasons. The following were recommended:

- Most respondents (7.7%) recommended that ICT equipment cost should be reduced to enable organizations fix the relevant security gadgets without running much of their budget on ICT the expense of other integral services of the organizations

- Personnel should be well trained to equip them with the necessary skills to handle ICT security related issues with confidence (7.7%).
- Anti-virus software should be upgrade on a regular basis to counter the malicious programs being developed from time to time by those bent on frustrating ICT users. Such upgraded software should have the capacity to self-delete any malicious program or worm introduced in the system.
- A further 7.7% suggested limiting internet access. For instance if one is seeking information on Information organization, so should that be. No room should be given to the searcher to wonder into other aspects for this might provide an opportunity to commit cyber crime. On this issue, others were of the opinion that only a limited number and particular staff should surf the Internet on behalf of other users. This will enable detection of the problem and its cause or the person who used the facility last.
- Another 7.7% recommended the development of an effective security policy to safeguard and preserve electronic information and its infrastructure from damage by both natural and manmade forces.
- To avoid viral infection of the information systems, 3.8% response advocated for discouragement of foreign diskette use. This will ensure system integrity and should any problem arise then it is internally caused and it can be easier to arrest. A further 3.8% suggested online processing as a measure. This might be a solution to reducing work backlogs but not necessarily a solution to ICT problems. Far from it, it makes the facilities prone to more threats due to the importation of programs from other organizations.

- The remaining 3.78% suggested burglarproof buildings to provide physical security to information resources.
- Another possible recommendation that is not captured in the above figure but prominently featured in responses and literature review is the classification of information into particular classes. Adjectives such as very sensitive, sensitive, confidential etc should be used. Where this is the situation, only authorized staff members can access the information or critical computer servers. This will enhance ICT and the information security.

4.45 PART TWO: ELECTRONIC INFORMATION USERS/ CLIENTS

Part Two of chapter IV is presentation and data analysis of ICT user's response. It is based on the research questions administered to users. The research questions are on the general user and organizations bio data, organizations used, knowledge about organizations' existence and services offered, types of ICTs used, security related threats and solutions to the threats.

4.46 Category of organization.

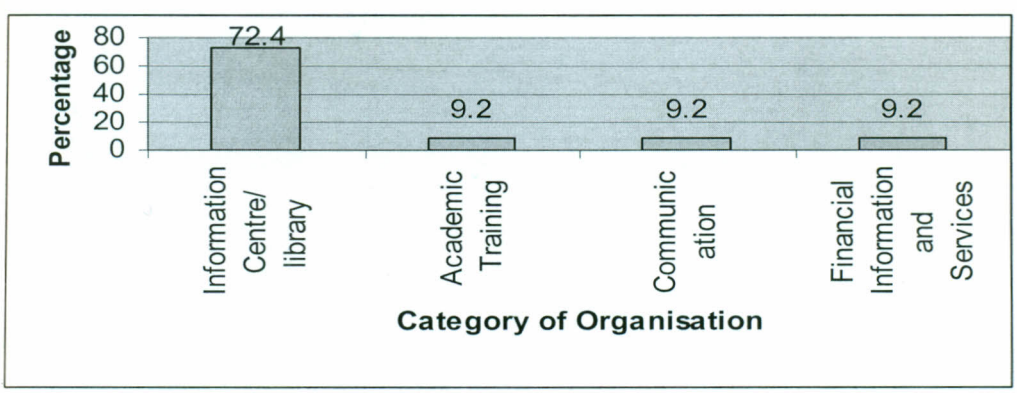

Fig. 34: Category of organization

The bulk of users interviewed make use of information centers and libraries. This accounts for 72.4% while 9.2% of users made use of training, communication and financial institutions. This is attributed to the fact that most ICT users visit Information centers purposely to satisfy their information needs. It may also be due to the fact that most users who are students have little to do with financial and other organizations.

4.47 Gender of respondents

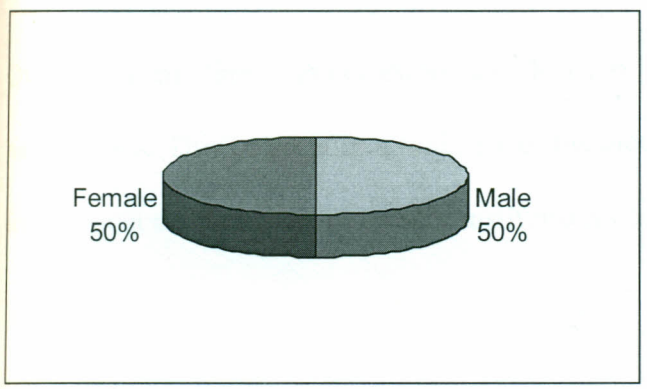

Fig. 35: Gender of respondents

The sampling was done such that half of the respondents are male and half are females thus having a gender balance.

4.48 Nationality of Respondent.

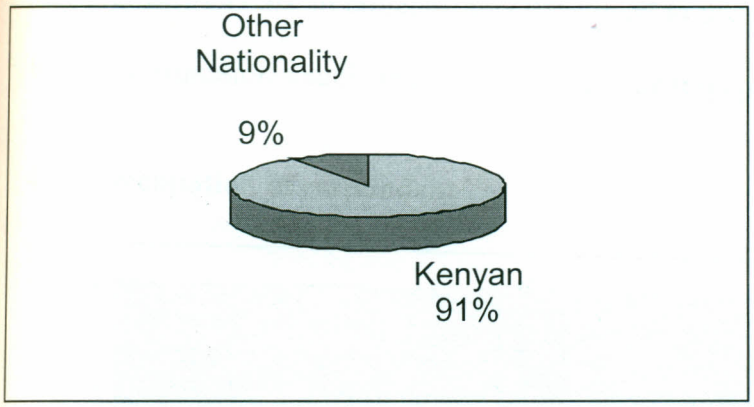

Fig.36: Nationality of respondent

Over 90% of those interviewed are Kenyan nationals with the rest being other nationalities. This is because a majority of the electronic information users in Nairobi are locals, most of whom are in tertiary institutions concentrated in the study area.

4.49 Age of Respondents

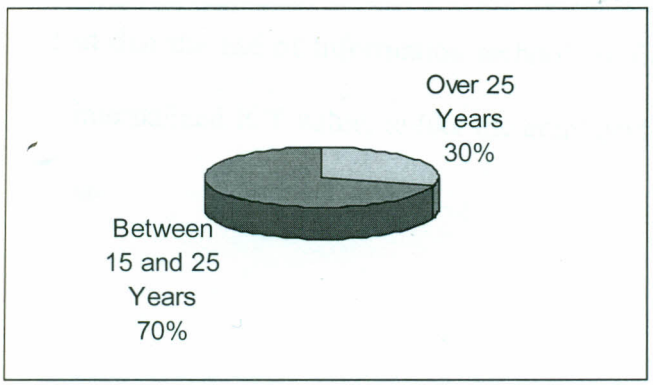

Fig. 37: Age of respondents

Of the electronic information users 70% were between 15 and 25 years and 30% were over 35 years. The younger generation of ages 15-25 years are more keen and conversant

with ICTs as opposed to over 25 year olds. As already pointed out, this is an age in which most users are in colleges hence the need to use ICTs becoming almost inevitable in their information search and general communication purposes.

4.50 Occupation of respondent

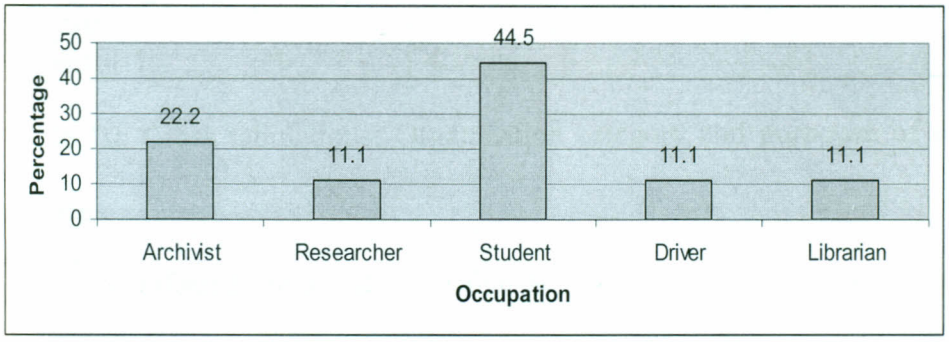

Fig. 38: Occupation of respondents

Out of the whole population studied, students accounted for 44.5% of respondents and 22.2% were Archivists dealing with storage and retrieval of information. The rest of the respondents were drivers, librarians and researchers consisting of 11.1% each. It is evident that the use of Information technology for students seems a must. As such, they have internalized ICT value, unlike the employed users who only use it when it is a must to do so.

4.51 Cross tabulations: Organization category and purpose of using information service

	Surfing the Internet	E-mail Services	Surfing for research and Email Services	Email & Telephone	Email and Banking Services	Email, Goods Purchasing and Telephone	Email, Banking and Telephone Calls
Private					1		
Public	1	1	4			1	1

Table 10: Cross tabulations: Organization category and purpopse of using information service

It can be inferred from Table 10 that ICTs in most public organizations are used for internet surfing, e-mail services, banking, goods purchasing and telephone service as opposed to private organizations.

4.52 Accessibility and services used.

4.53 Organization interacted with in electronic information and user service utilization

	Frequency	Percent
Information Centres	1	8.3
Telecommunications	1	8.3
Information Centres and Banks	1	8.3
Information Centres and Cyber Cafes	6	50
Information Centres, Telecommunications and Cyber Cafes	1	8.3
Information Centre / Library	1	8.3
Academic Training and Research	1	8.3
Total	12	100

Table 11

Most users interacted with all categories of organizations studied save for banks or financial organizations. Of the total organizations interacted with by users, Information

centers and cyber cafes recorded the highest level of user interaction with electronic facilities and or information. This is because of their realization that they have information gaps that must be bridged or filled, hence the high frequency to information organizations. A lesser number made use of banks and telecommunication centers since the majority of the users had no business with the banks as their economic status did not allow them to. More so, due to liberalization of communication industry, services that were hitherto provided by telecommunication institutions are now available in the alternative competitors such as information centers and cyber cafes. There is therefore little need to visit conventional communication organizations.

4.54 Ways of knowing organizations' existence

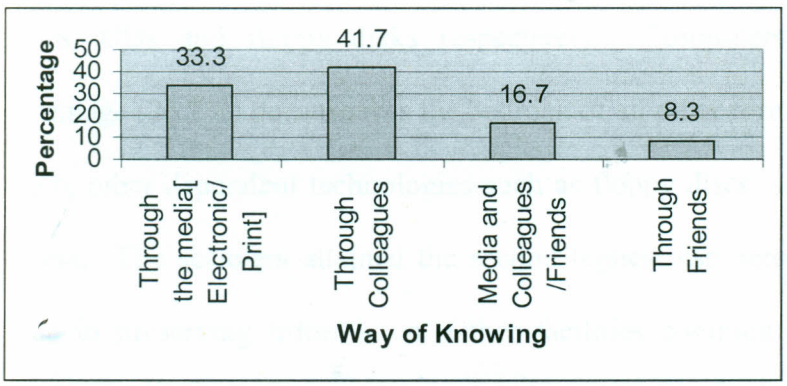

Fig. 39: Ways of knowing organizations' existence

The commonest way of knowing about the existence of information organizations used was through colleagues. About 41.7% of all the users indicated that they knew about the organizations through colleagues. A further 33.3% knew about organizations existence through the media i.e. both electronic and print. Another 16.7 %8.3 knew through the

media, and colleagues or friends. Only 8.3% new about the organizations through friends.

4.55 ICT types used

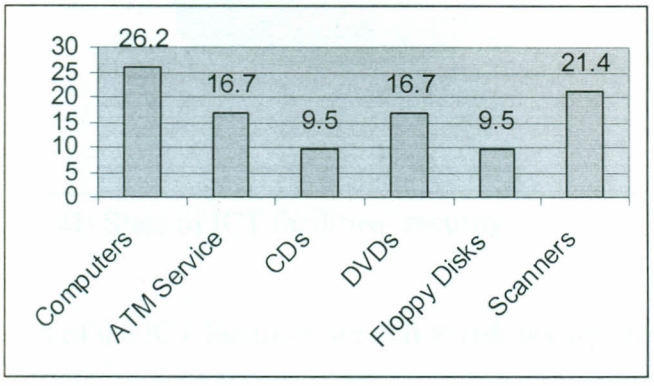

Fig. 40: types of ICT used

Computers were the most common type of ICT used followed by scanners, ATM service DVDs, CDs and floppy disks respectively. Computers recorded the highest use percentage (26.2%) because it is the bedrock of all other forms of the technology, without which, other dependent technologies such as floppy discs, scanners etc will be rendered useless. The scanners attained the second highest use percentage (21.4%) due to their value in preserving information. Other facilities commonly used include; ATMs and floppies and CDs. They attracted 9.6% usage.

4.56 State of ICT facilities' security

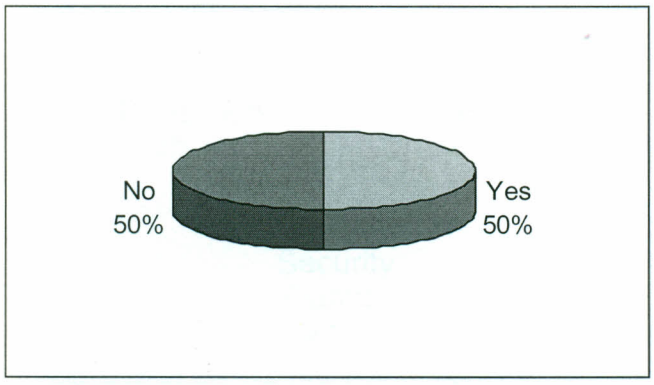

Fig. 41: State of ICT facilities' security

Half of the ICT facilities are still at risk because they are still not secured.

On whether or not the ICT facilities are secured, the response was50% to the affirmative and 50% to the negative. For those who responded to the affirmative, they cited strict use of PIN numbers, passwords and the user IDs to access electronic information. To counter viruses, anti virus software are used to scan and delete any virus detected in the systems. Others mentioned restricted access policies, non-usage of foreign diskettes, round the clock surveillance and secured buildings beefed up with 24-hour security guards. Those who said that the ICTs were not properly secured argued that despite the measures in place, members of staff could cause harm to the information systems for malicious reasons. It is not uncommon to hear of physical destruction of the computer servers by those entrusted to take care of the same. Besides, though supervision of use is a measure of security, any lapse can lead to ICT misuse and or corruption of data.

4.57 Types of security used

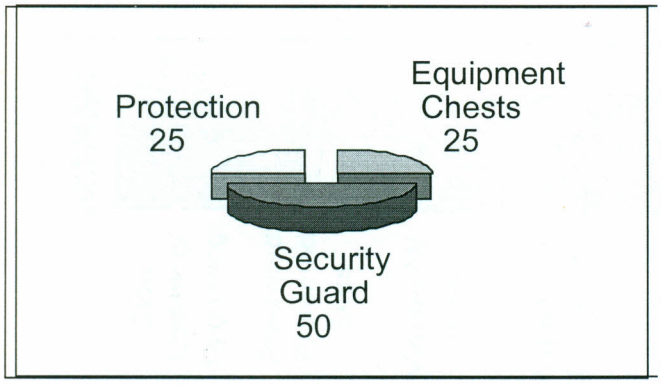

Fig. 42: Types of security used

Security Guards were used in 50% of the organizations to guard against electronic information and facilities. Antivirus protection and equipment chests used accounted for 25% user response in each of the organizations used.

4.58 Rate of users experiencing problems while using ICTs

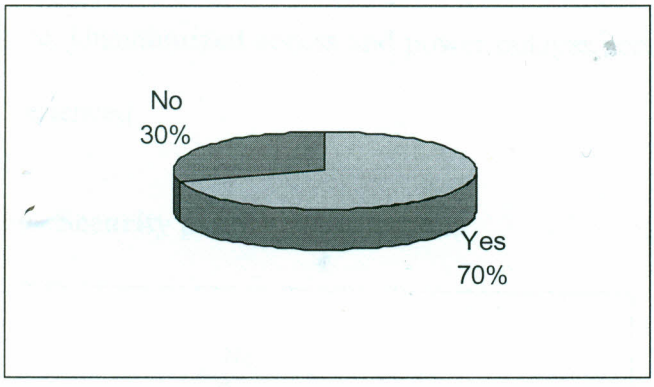

Fig. 43: Rate of users experiencing problems while using ICTs

A high number of users confirmed that they experienced problems with the use of Information Communication Technology. This was 70%. Only 30% of the users did not experience any problems when using ICTs.

4.59 Problems experienced in ICT usage

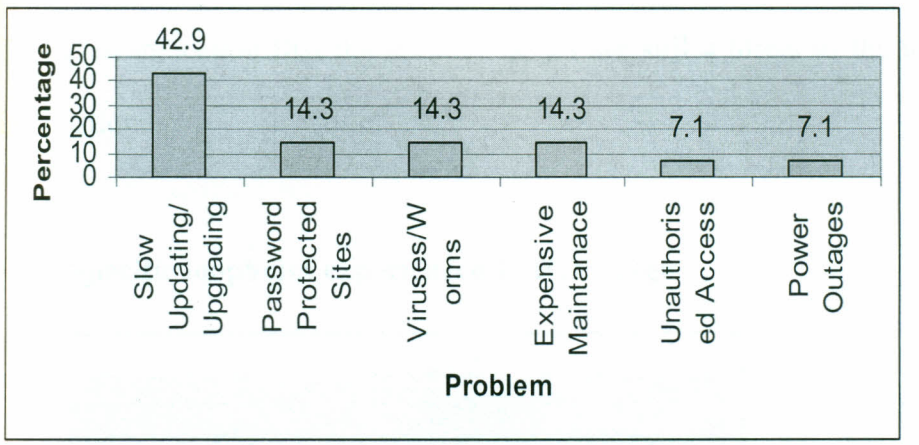

Fig. 44: Problems experienced in ICT usage

The major problem encountered when using ICTs was slow upgrading/ updating accounting for 42.9% of the problems encountered. Password protected sites were cited as a hindrance to the usage of ICTs accounting for 14.3%. Viruses and expensive maintenance of facilities accounted for 14.3% each, for the problems experienced in usage. Unauthorized access and power outages accounted for 7.1% each of the problems experienced.

4.60 Security problems/limitations

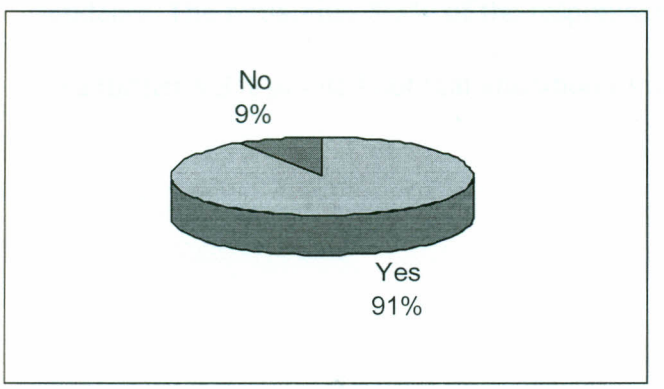

Fig. 45: Security problems/limitations

It was almost unanimous that users have experienced security lapses in the use of ICTs. 91% of the users confirmed so. Only 9% of the users said that the resources were secure. This is an indication that the security lapses are still a threat to the usage of electronic information.

4.61 Specific loopholes experienced in ICT usage

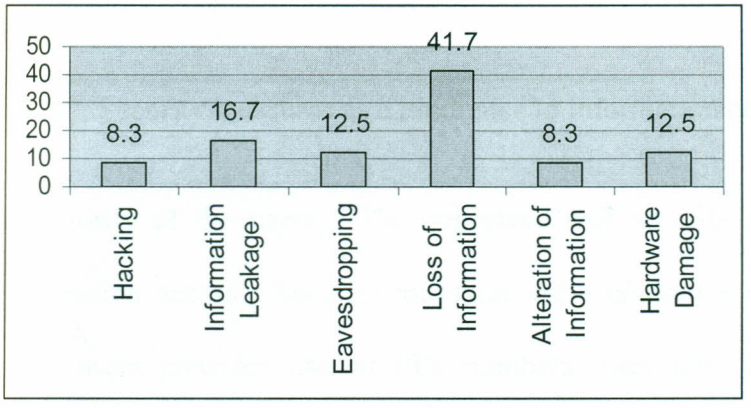

Fig. 46: Specific loopholes experienced in ICT usage

From the figure above, the greatest loophole that ICT users experienced is loss of information, which accounted for 41.7%. Eavesdropping and hardware obsolescence accounted for 12.5% each. As a loophole, information leakage was cited by 16.7% of the respondents. The remaining 8.3% of the respondents cited hacking as the main weakness while a further 8.3% pointed out that alteration of information was the main shortcoming.

4.62 Security measures as a hindrance to information access

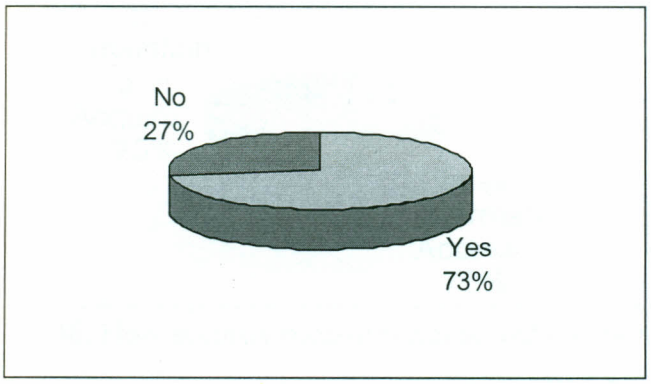

Fig. 47: Security measures as a hindrance to information access

A majority of the users, 73%, concurred that security measures were a hindrance to information access. Security measures are a hindrance to information access because: some users consider use of PIN numbers, user IDs, and passwords as being user-unfriendly as they establish a form of bureaucracy. Besides, it is quite easy for such numbers to be forgotten. Signing in and out of user register is in itself a hindrance. Restricted access robs the users freedom to navigate the entire databanks to look for required information. All these translate into unnecessary time wastage and make the whole exercise quite expensive. See figure below to illustrate the above.

4.63 How security measures hinder information access

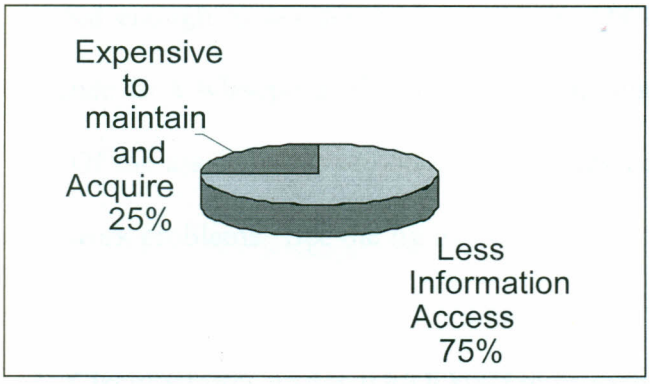

Fig. 48: How security measures hinder information access

The figure above shows that 75% of the respondents had less information access problems due to the security measures put in place. For instance it is difficult for users to access information if the password is kept secret. Others argued that security measures are a problem because of being costly and expensive to acquire and maintain.

4.634 Assistance given by organization staff

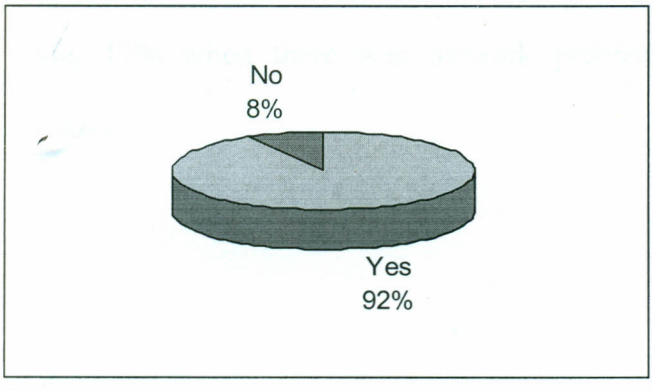

Fig. 49: Assistance given by organization staff

Only 8% of the users received little or no assistance from the organizations' staff. They however do not indicate whether it was due to in- competencies of the staff in ICT or

negligence of duty on the part of the staff. However one can infer that the users were equipped enough to ask for staff assistance. On the other hand the organizations gave assistance to a whooping 92% of the information users accessing the service through them. Of the assistance given 58% was on data access, 25% on system failure and 17% on network problems. See the figure below.

4.65 Circumstance under which staff gave assistance

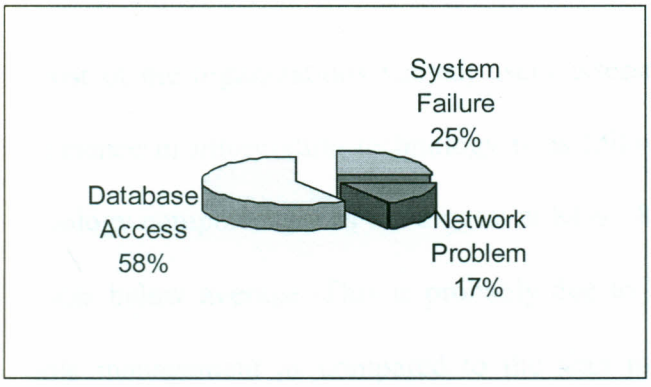

Fig. 50: Circumstances under which staff gave assistance

On circumstances under which users were assisted, 25% were assisted during system's failure, 17% when there was network problem and 58% were assisted to access databases.

4.66 Level of staff experience on electronic security systems.

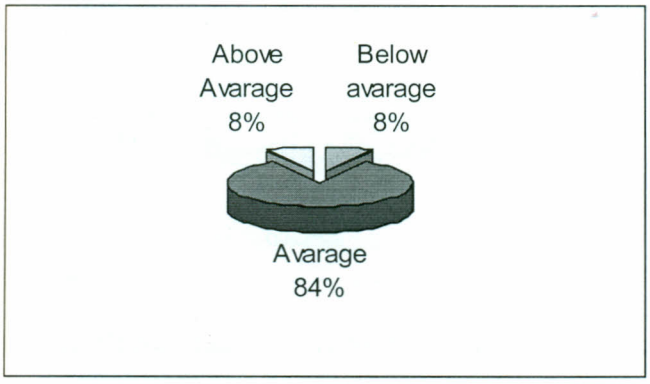

Fig. 51: Level of staff experience on electronic security systems

In most of the organizations visited, users assessment and or rating of staff ability and competence in information technology is as follows; the staff rated as being average in technology competency was the biggest at 84%. 8% was above average whereas another 8% was below average. This is probably due to the fact that most ICT staff are in the middle management as compared to the lean top management and the lower cadres, perhaps the support staff both of which accounts for 8% respectively. The lower cadre perform routine work hence their poor ICT skills. This experience demonstrates that in most organizations, the staff is ill equipped technologically and therefore not qualified to handle electronic information facilities and or protect the same from threats that may befall them.

4.66 Recommendations for possible security measures.

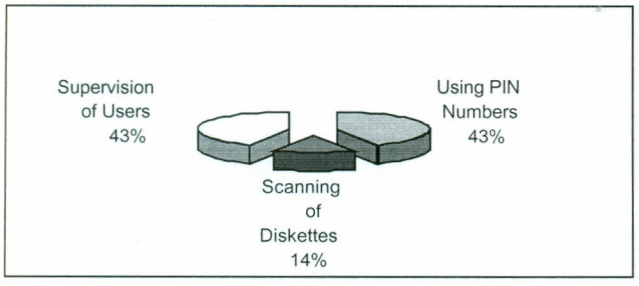

Fig. 52:Recommendations for possible security measures

Of the respondents interviewed, 43% of the users suggested use of PIN numbers and passwords all of which must be unique to every user.

Another 43% recommended round the clock surveillance and supervision to guard against insecurity of the resources. Only 14% suggested scanning of foreign diskettes. It thus emerges that user supervision and use of identification numbers and passwords is a good measure to secure information.

4.68 PART THREE: ICT VENDORS AND/OR DEALERS

This is the last part of presentation and data analysis, which targets the ICT vendors. The main issues discussed includes:- respondents, bio data, organizations bio-data, affiliation (if any) to other organizations, types of ICT facilities dealt with, threats to electronic systems and recommendations or suggestions to address the threats.

4.69 Respondents' bio data

4.70 Age of respondents

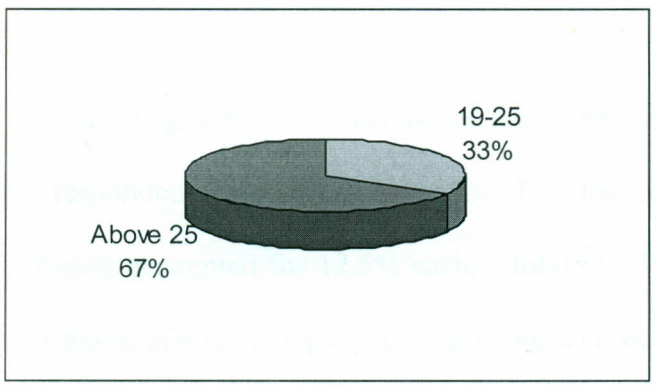

Fig. 53:Age of respondents

As opposed to the ICT users, the majority of whom were between 15 and 25 years old, 67% of the ICT vendors interviewed were above 25 years and only 33% were between 19 and 25 years. This is because unlike the users, to be employed in any firm, one has to be over 18 years of age, hence the high rate of ICT vendors being above 25 years of age. Besides it is most likely that people at age 25 years and above are through with academic and professional training therefore this explains why almost three quarters of the population interviewed was above 25 years of age.

4.71 Occupation of respondents

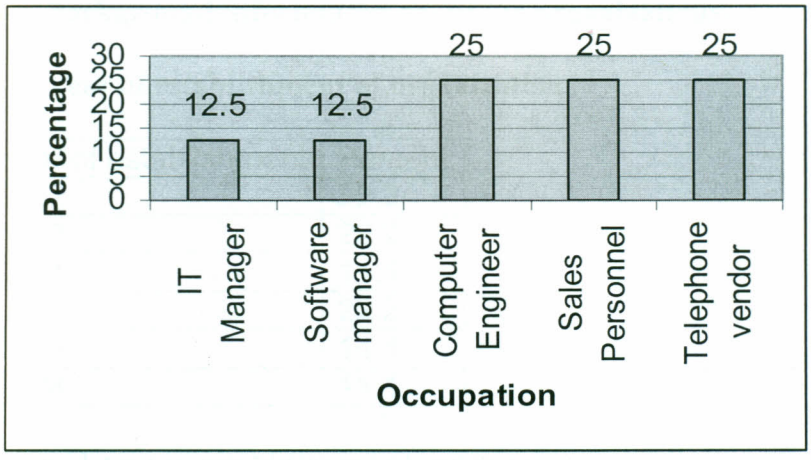

Fig. 54: Occupation of respondents

Computer engineers, sales personnel and telephone vendors accounted for 25% each of the respondents amounting to 25%. For the management cadres, IT and software managers accounted for 12.5% each, a total of 25%. About all the respondents mistook their designations in employment as being their occupation. Instead of showing that they are vendors, they talked about their position in employment. This is because most employees hardly distinguish between occupation and designation. If anything, they use these terms interchangeably.

4.72 Background information about the organizations.

4.73 Year of establishment of organization

Year of establishment	Percent
1952	22.2
1988	22.2
1991	11.1
1998	22.2
2003	11.1
2004	11.1

Table 11:year of establishment of organization

Information Technology vendors were established as early as 1952 and others as late as 2004. These organizations have offered IT services and facilities in the country over the years.

4.74 Objectives of organizations

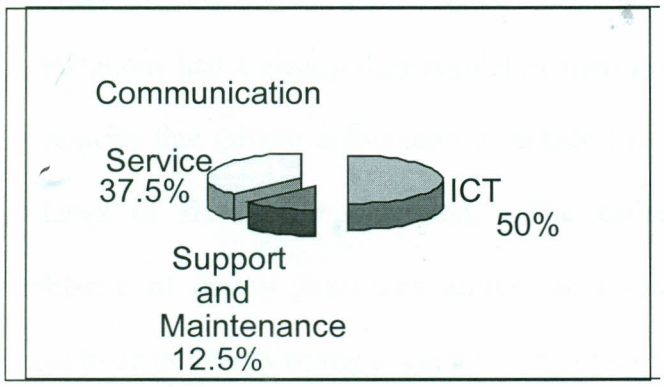

Fig. 55: Objectives of organizations

ICT Sales was the leading objective of the organizations at 50% with communication services coming second with 37.5%. Support and maintenance was cited by 12.5% as an

objective of the organizations. Thus the vendor organizations were established with varying objectives.

4.75 Policy regulating organizations' operations.

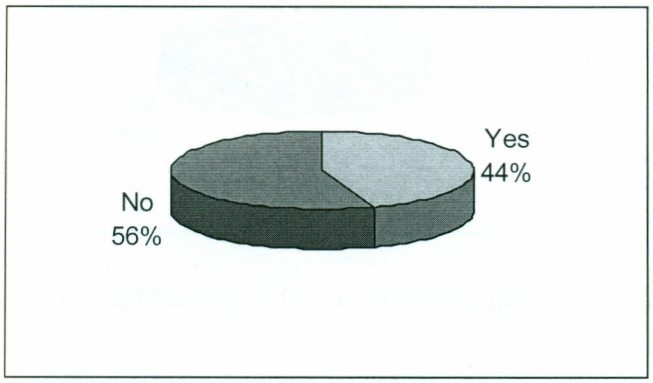

Fig. 56: Policy regulating organizations' operations

The researcher wanted to know if the organizations had any formal policy regulating operations and by extension to find out if the said policies factors in the elements of ICT security and to what extent. The researcher to find out that there was no policy regulating the organizations' responsibilities in 55% of the organizations. Only 44% of the organizations had a clear policy regulating their responsibilities and operations. Some of the policies that govern organizations include UK Copyright Law of 1985, City Council By-Laws of fixed-point operation. The earliest established organizations had a semblance of policy guidelines unlike the recently established organizations, which seems to be in a hurry trying to get a footing in the turbulent economic waters of Nairobi.

4.76 Affiliation to other organizations locally and internationally.

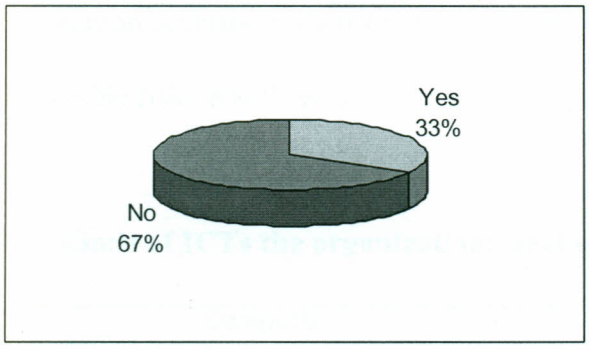

Fig. 57: Affiliation to Local/International organizations

Only a few of the organizations, 33% are affiliated to other organizations both locally and internationally while 67% of the organizations are independent and have no affiliates at all. The affiliation to or lack of it is determined by whether the organization is multi-National or indigenous.

4.77 Services offered by the organizations.

4.78 Components of Information security captured in the ICTs

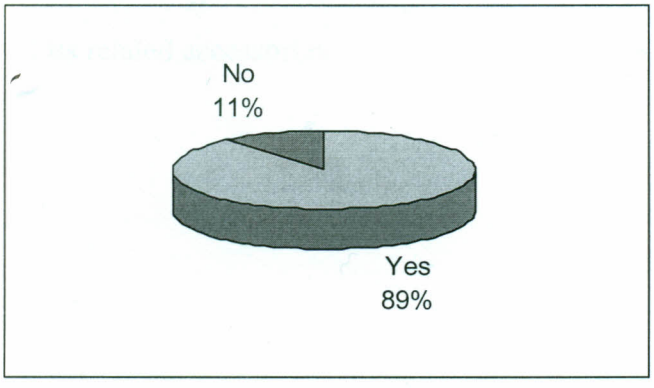

Fig. 58:Components of information security

The component of information security was captured in an overwhelming 89% of the ICT vendor organizations. Only 11% of the vendors have not captured the element of information security in their operations therefore exposing their facilities and information to possible risks and threats.

4.79 Kinds of ICTs the organizations deal with

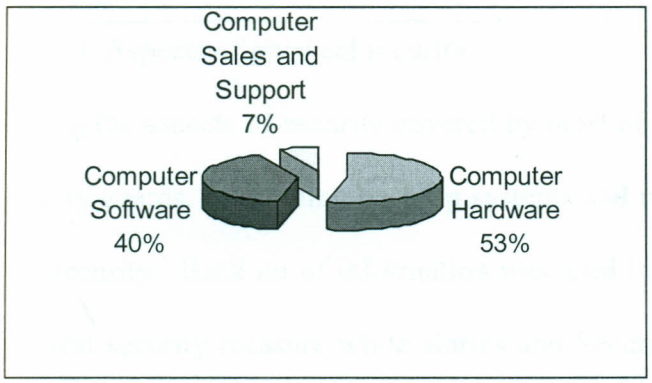

Fig. 59:ICTs dealt with

Computer hardware accounted for 53% of the ICTs that vendors deal with. Computer software and computer sales and support accounted for 40% and 7% respectively. This implies that majority of the ICT vendors' operations rotates around the axis of computers and its related accessories.

4.80 Aspects of physical security covered

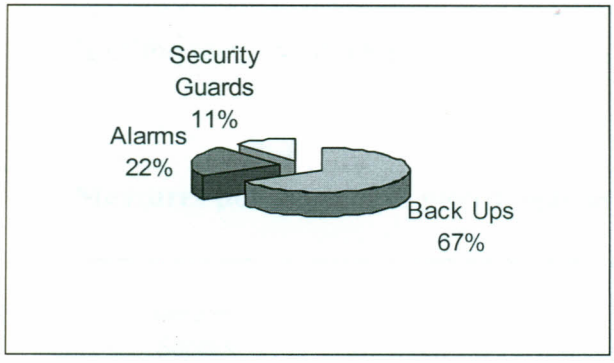

Fig. 60: Aspects of physical security

Among the aspects of security covered by most of the organizations were employment of security guards, developing back up systems and use of alarm systems to detect any sign of insecurity. Back up of information was used in 67% of the vendor organizations as a physical security measure while alarms and Security guards were used in 22% and 11% of the organizations respectively.

4.81 Other aspects of systems security

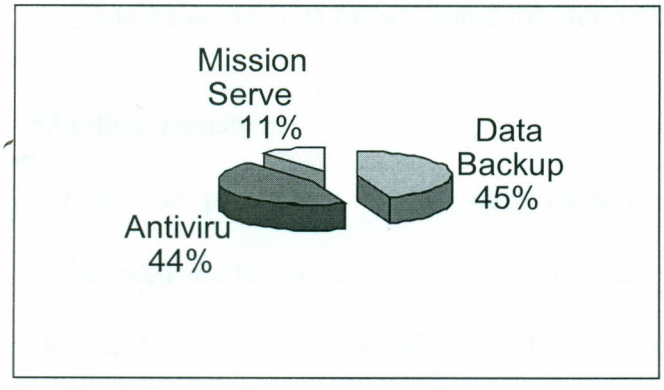

Fig. 61: Aspects of systems security

Of the system's security covered, data backup accounted for 45% and anti-virus 44% respectively. The remaining is the mission critical server of the systems, which accounted for 11% of the security components.

4.82 Measures put in place to guard against insecurity.

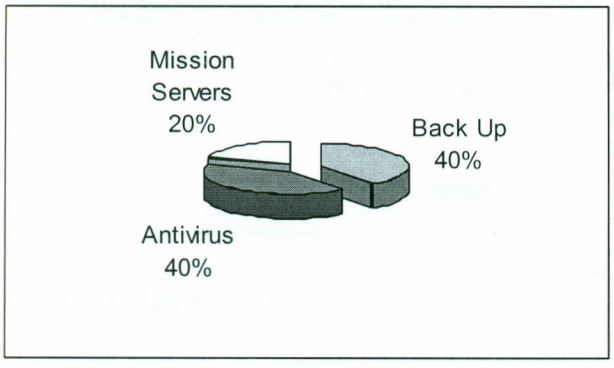

Fig. 62: Measures against insecurity

From the response on possible measures, both data backup and anti-virus installation recorded 40% while mission critical server registered 20% respectively. Thus the measures put in place to guard against systems' insecurity are backup of information, anti virus installation such as firewalls and mission critical servers.

4.83 Other measures

They include passwords, which were recommended by 47.6% of the respondents. Another measure to safeguard the ICTs physically is the use of security guards. This was endorsed by 28.6% of respondents. Burglarproof facilities were cited by 14.2% as another possible measure to guard against physical threats. Finally, anti-virus software use and assigning of computers to specific people for accountability purpose was cited as

measures by 4.8% each, for the vendors who completed the questionnaires. See the figure below for illustration.

Other measures

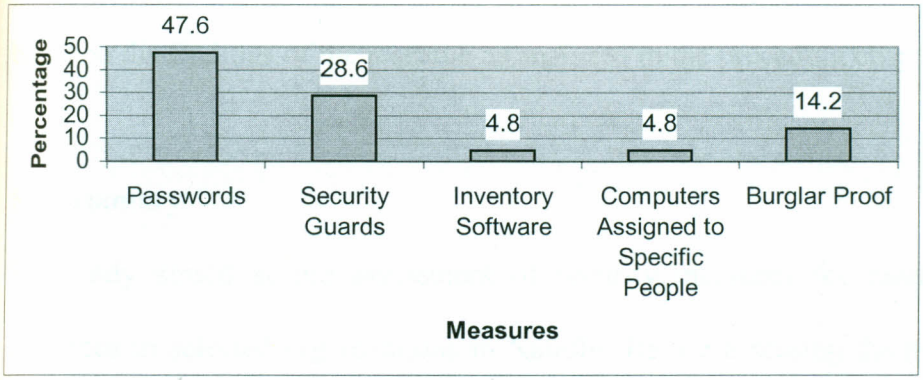

Fig. 63: Other measures

4.84 Recommendations

The recommendations suggested by ICT vendors are not different from the measures they suggested. For instance, most respondents recommended use of passwords, security guards, assignment of computers to specific people, installation of antivirus software, data back up and use of facilities to check against both logical and physical security. By extension these recommendations are in agreement with those recommended by ICT specialists and users.

CHAPTER FIVE

Summary of the main findings, conclusions and recommendations

This chapter attempts to summarize the integral issues of the study and recommendations based on the findings of the research as analyzed in the preceding chapter.

5.1 Summary

The study aimed at the assessment of security measures for electronic information resources in selected organizations in Nairobi. Before assessing the measures, the study established or identified some of the threats that electronic information is faced with. Three main types of respondents were targeted viz ICT specialists, users and vendors.

The main issues discussed in the study are:

- Types of information communication technologies:
- How the facilities are used
- Security policy aspects covered
- Security measures against internal threats and external threats
- Physical media security
- Safety measures for information storage media against:

- Environmental conditions
- Physical damage
- Obsolescence
- Vandalism
- Floods

- Fire
- Wars and terrorism
- Other perils

➢ Confidentiality of:

- Electronic by products
- Telephone accessories

➢ Safeguarding information against:

- Eavesdropping
- Masquerading
- Interception
- Dubbing

➢ Ensuring information reaches intended recipient

➢ Secure use of ATM and other related electronic cards

➢ Protection of clients' privacy

➢ Protection of client's money against fraud

➢ Disaster preparedness and recovery

➢ Other problems of security

5.2 Types of organizations

Most organizations are founded upon statutory policy documents, which regulates their operations. The organizations studied are basically information, academic, financial, communications and research and data processing organizations among others. The common denominator among them is that they all use ICTs for their day-to-day operations. Some of the ICT equipment used include computers, telecommunication

accessories such as satellites, fax machines, telephones etc. Other equipment used are scanners and microfilms, information storage facilities such as floppies, CDs etc. These facilities are used for data communication, e- transactions, archiving purpose, general office work among other uses.

5.3 ICT Policies

Majority of organizations have ICT policies in place. The GIS (Government Computer Service) formerly the Government Computer Centre for instance has a policy, which ensures that standards are adhered to. The policy gives right specifications for computers and related accessories. Besides, it ensures that the government is kept abreast of considerable technological advances taking place in the most cost effective manner.

The organizations' security policies factors in the issues of electronic information security because of its vulnerability to threats. Aspects of security covered are physical security and systems security (software and data security). Issues such as hardware security, data or information security against corruption and manipulation are captured in the policies.

5.4 Security Measures against:

(i) Internal threats

To guard against this aspect, the ICT room should be physically secured. ICT room should be restricted to IT personnel only and be a no go zone for other members. There should be backups, of soft and hard copies kept in fireproof safes preferably in remote locations. More still, use of external or foreign diskettes should be discouraged as much

as possible. Personal computers should have anti virus programs to filter any virus if detected. Network security can be maintained through the use of fiber links and or firewalls to police both intranet and internet links. Data access should be password, ID and administration rights centred.

(ii) External threats

To safeguard the interest of an organization, only one computer should be connected to the internet and all email attachments should be scanned. Data should be encrypted or scrambled to ensure that only authorized personnel gets access to it.

5.5 Ensuring confidentiality

To enhance confidentiality, office should be job specific. There should be designated personnel for particular duties e.g. procurement, finance, administration, records etc. Besides, waste paper or extra products of sensitive data should be shredded or pulped. In the Government Service for example, hard copies of payrolls are destroyed by shredding and pulping. Printouts are shredded at the central place located in the treasury building.

5.6 Telecommunication security: telephones and related accessories

As suggested by respondents from telecommunication organizations, installing a manual PABX for telecommunication call filtering can ensure telecommunication security. The PABX is also handy in checking against eavesdropping. Besides, electronic surveillance of phone use is recommended as a measure. Interceptors and dubbers can be countered by

use of scrambled or encrypted messages as does security organizations to conceal their communications; only an insider can make sense of their conversations.

For masquerades, the telephone operator should always seek user details and refer to the internal documents before allowing communication to take place. Where the caller is doubted, then the operator should cancel the call. Security for analog based system is achieved through spread spectrum technology. This involves frequency hopping. A given channel may be hopped from frequency to frequency to avoid the above problems.

5.7 Data/information transfer

To ensure that information is used for intended purpose and not any other activity, the information is encrypted (secret coding of information is done). This is by use of a key or secret strings of digits to secure the information. Only the intended recipient who knows the secret formula of decryption can therefore access information.

5.8 ATMs and related electronic cards

To protect users from fraud, cryptographic functions are preferred i.e. confidentially and authenticity. The purpose is to authenticate the cash withdrawer and debit account accordingly. This is part of security data transfers; issues scrutinized are passwords, PIN numbers, signatures and photos of the account holder.

Clients' privacy and avoiding of unauthorized access can be ensured by use of customer IDs, PINs and bank account numbers. Besides, the ATMs should be located in private

areas to avoid exposure. What is more, access methods should be modified upon such that retinal and finger prints scan is undertaken to ensure identity of the withdrawer. In addition, use of body-installed clips can add value to the identification and verification process.

5.9 Electronic money transfer

In case of electronic money transfers from one point or person to another, the safety measures include inter Bank telephoning so that the recipient can withdraw cash from the bank within his vicinity as the telephoning Bank arrange to pay the other bank later through their established channels. Alternatively, keywords or statements known only by the sender and intended recipient are used to authenticate the recipient of the cash. The sender of the money asks a question and provides answer details known only by the intended recipient. Once the financial institution confirms that the answers given by recipient are in agreement with the sent details, payment can be made to the person. This is because his identity i.e. ID card and the details given are the same as those given by the sender. For instance, questions such as "what is the name of the sender's 1st born?" are asked. Once the recipient gives the right answer, he can cash the money.

5.10 Physical media security

The ICT physical security can be assured if access to the area is restricted only to the ICT personnel. The computer room should always be under key and lock. Only designated personnel should handle computer room keys. Above all, computer areas should be secured by burglarproof facilities. They should be installed with metallic doors and

grilled windows. The Euro-bank computer destruction could not have happened if these measures were in place.

5.11 Information storage media and problems faced

To guard against environmental deterioration, the ICT room should be air-conditioned. The CDs, DVDs and other media should be kept in special containers and locked in cabinets and the room should be kept clean all the time.

For physical damage due to heavy usage, legal back-up copies should be made. It is preferable to use copies and preserve the originals for a rainy day.

Technological obsolescence is a headache in the field of technology. To address this problem, scanning, migration and emulation of information to new storage media whenever there are signs of obsolescence is recommended. Upgrading and or purchase of new fashions cum replacement of obsolete technology are called for. This should be done from time to time depending on technological advancements.

Vandalism is checked through burglar proof and secure computer rooms and offices. They should be equipped with a 24-hour round the clock surveillance by close circuit monitoring cameras and security guards. As pointed out already, they should be declared restricted and no go zones by everybody save for IT staff. Closely related to vandalism are wars, terrorism and riots. These problems are only addressed by the state security

department, which has to ensure law and order and protection of its sensitive installations from the stated threats, be they by internal or external aggression.

To address flood related threats, flood proof measures should be put in place. ICT facilities should always be installed in the upper rooms that are preferably water tap free and have leak proof ceiling environment.

Finally, fire as a peril can be addressed through construction of fireproof ICT rooms. Where this is not the case, precautionary measures should be taken such as installing fire fighting equipment e.g. fire extinguishers, fire and smoke detectors, fireproof cabinets among others. Computer rooms should be declared no smoking zones and staff should be drilled regularly on how to fight fire in case it occurs.

Other problems associated with electronic information security are information leakage, reproduction of valid messages through invalid circumstances (replay), inadequacy of copyright law, and difficulty to supervise and or monitor staff on ICT usage. These problems can be addressed by ensuring that the already stated measures and recommendations here under are put in place.

5.12 Recommendations

The recommendation made below are a summary of what ICT vendors suggested as measures to counter the various threats facing ICTs. They include:

- Buildings that can withstand bombs, burglary, fire, floods and other perils should be constructed for ICT facilities.
- At no time should external floppies or disks be allowed into the system as they may be virus carriers. If they have to be used, then they must first be scanned before being put into the computer system.
- Secure internal connectivity with integrated firewalls should be established to check against logical threats.
- Disaster preparedness, management and recovery plan should be developed and upgraded or revised from time to time by organizations using ICT in their operations.

5.13 ICT USERS

The majority of users are between ages 15 and 25, a school and college characteristic age bracket. They make use of electronic facilities at information centers, telecommunications and banking organizations, which they knew about mostly through colleagues and the mass media.

Most users confirmed they use ICT facilities such as computers, telephones, floppy diskettes, internet etc for research, email service, communication and other integral purposes.

5.14 Security of facilities and security related problems to users.

Opinion as regards the security of the facilities was fifty fifty for and against. Most of those who said that the facilities were secured cited strict use of PIN numbers, passwords and user IDs among other observations. Those arguing that there are information security lapses cited loss of information leakage, eavesdropping, hardware damage, hacking and alteration of information

As regards problems associated with using ICT, 70% of the users cited slow upgrading or updating as a problem. Others argued that password protected sites are difficult to access and ever occurring power outage and fluctuations is in itself a problem encountered by many users. This causes unnecessary time wasting.

5.15 Assistance from staff

Most of the users were assisted in the technology use. They were assisted in accessing the database and incase of system or network failure. On the ratings of staff technology competencies, it emerged that many staff members were averagely competent, hence the need for more training to equip them with skills to handle technology.

The user's recommendations are in agreement with those made by ICT specialists. They recommend measures such as use of PIN numbers and passwords, scanning of foreign diskettes and if not discouraging their use completely.

5.16 ICT VENDORS

These are organizations dealing mostly with ICT sales and promotions. Most of the respondents interviewed were above 25 years of age since they are the majority in the employed bracket.

5.17 Security policies

In the organizations studied, 44% had policies to regulate their operations and functions. Such policies had captured the element of electronic information and infrastructure security. Some aspects covered include the use of security guards, development of backup and alarm systems to cushion technology against any insecurity.

5.18 Measures in place to check against

(a) Physical insecurity

- use of burglar proof offices
- Access to warehouse restricted
- Motion detection systems.
- Locks and alarm use

(b) Systems insecurity

The ICT vendors suggested the improvement or installation of the following:

- In built anti virus software's which are self-deleting incase of a virus.
- Use of firewalls (installed on file server) and certificates of authenticity i.e. PIN numbers, passwords and use IDs.

Thus the vendors are in agreement with the specialists and users of ICTs as to what should comprise security of electronic information.

5.19 Threats

Threats to electronic information are highly complex. From the three groups of respondents studied and literature reviewed, the researcher established the following findings as regards threats to electronic information.

5.20 Ulterior driven motives

Some users access the internet with the purpose of destroying or stealing any information they come across. Often this results into great loss to an organization.

5.21 In-genuine users of ICT

Whereas there are some users who genuinely use information facilities and the information transmitted therein genuinely, there are others who take advantage of ICT to commit computer crimes. Such crimes comprise data corruption, inappropriate contents, espionage and sabotage. Others are leakage, impersonation, masqueration and repudiation. This breed of threats thrives well in a networked environment that allows the spread of virus, which infect many systems before being detected.

5.22 Infrastructure crippling.

Some organizations experience network jamming, which are artificially,

caused (denial of service). This is what is known as malicious unavailability

of network. This scenario is equivalent to frequency jamming of airwaves in case of radio or television transmission. This was the case between two local FM stations which traded insults over airwaves interference. The Kiss 100, complained loudly about Radio citizen malice in crippling its airwaves for a full weekend in which Kiss 100 was unable to be on air.

5.23 Malicious programs

These are man-made programs that attach themselves to other programs to be executed. They end up destroying and or altering the existing data by adding new unnecessary data. They also install software that may lead to system collapse.

5.24 Privacy violation

This is where third parties acquire personal information on freely given data from the web, read and even copy to a remote system.

5.25 Hacking

Hackers use Trojan Horse virus i.e. a program, which combs personal computers or networks for confidential files. Often they come as email attachments, capable of opening a backdoor entry into a computer system to access and compromise private information.

5.26 Corporate humiliation

In an event that an organization is attacked, the resultant effect is corporate humiliation. This explains why some organizations were skeptical and reluctant to allow this study to be undertaken since they viewed it as business competitor sponsored study whose results might be damaging to the reputation of the organizations.

5.27 Spamming

Thomas (1998.42) defined spams as the scourge of the Internet. Spams not only clog it but also add unnecessarily expense to the person down loading them.

5.28 Cyber terrorism

This is unlawful computer act whose objective is to influence or coerce an organization to conform to 'terrorists' ideals. As John Edwards, senator of North Caroline puts it, the damage caused by a keyboard and a modem are as serious as those committed via the gun or bomb (Daily Nation March 2005).

5.29 Masquerades

These are internet attackers who may pretend to be legitimate hosts. A web site within a similar URL, may be designed to defraud a company money or information on false pretence.

5.30 Unauthorized access

ICT information is always under constant threats from people who may want to access it without permission. Such people often have bad intentions of stealing, committing fraud, destroy and or corrupt data. Unauthorized access manifests itself through: eavesdropping, surveillance and industrial espionage.

5.31 Eavesdropping

This is tapping into communication channels to get information. Hackers mainly use eavesdropping to obtain credit card numbers.

5.32 Surveillance

This is whereby cyber criminals keep track of computer activities of other people. The information gathered may be used for sabotage or propaganda spreading.

5.33 Industrial espionage

This is whereby your business competitor or any other spies on your business strategies in order to finish you. This is done with an aim to get ideas on how to counter your plans by developing similar approach. In most cases, espionage as a cyber crime is committed by business competitors due to industrial competition reasons, disgruntled former employees of an organization, strangers who may stray into computer room or force entry

into computer through weak access points and network access in case the computers are networked or connected to the external world.

5.34 Computer errors and accidental access

This may be as result of people experimenting with computer features, which they are not familiar with. For example, a person may down load a file without knowing it is self installing and it is dangerous to the system. In addition, if end users have too much privilege that allows them to change or access sensitive files on the computer, then accidental access mistake may occur.

5.35 Tapping

This is whereby a person sends an intelligent programme on a host computer which sends him information from the computer. Alternatively, spying on a networked computer is done by special programs that are able to intercept messages being send and received by unsuspecting computers.

5.36 Cracking

This refers to the use of guesswork over and over again by a person until he or she finds or discovers a weakness in the security policies or software codes. Cracking may be done by individuals who have some knowledge of passwords or user names of authorized staff.

5.37 Piracy

This is the process of making illegal copies of copyrighted software, information or data.

5.38 Fraud

This is the use of computers to conceal information or cheat other people with the intention of gaining money or information. Normally, fraudsters are employees of an organization or outsiders who are smart enough to defraud unsuspecting clients. Fraud involves production or use of fake documents or development of computer programs to benefit a fraudster. For instance, an employee in a financial institution may develop an intelligent program which may credit his account with cents from other tax payers, depositors or bankers.

5.39 Alteration

This is illegal changing of data and or information without permission with the aim of misinforming the authorized users. This is usually done by those intend on hiding truth.

5.40 Physical threats

They include natural threats such as earthquakes and floods. Others are man induced e.g. fire and destruction out of malice as was the case when vital information together with its information communication technology, was crushed beyond recovery at the collapsed Euro Bank. Other threats include outbreak of wars, riots and terrorism i.e. as was the case

in August 1998 in Nairobi when terrorism was visited to the city, and the September 11 2001 attacks on the famous World Trade Centre and Pentagon in the USA.

Thus the threats are logical and physical. The logical threats include data corruption, sabotage, cyber terrorism, malicious programs, denial of service etc. The physical threats on the hand are man made and natural. Man-made threats are malicious acts, carelessness, riots, fires, wars, terrorism etc whereas natural disasters include phenomena such as floods and earthquakes.

5.41 ICT SECURITY POLICY

The overall objective philosophy of ICT security policy is to provide direction designed to ensure protection of data, information, application and systems. ICT security should be based on the following concepts.

- A secure computing environment is based on managing risks to an appropriate level. The security controls applied to a computer system should be commensurate with the magnitude of harm that would result from loss, misuse, inability to access, unauthorized access to or modification of the information in the system. A risk-based approach to security therefore promotes the use of limited resources wisely to protect most critical systems in a cost effective manner.
- Everyone should be responsible to ensure that ICT resources are not exposed to undue risks. Although managers and others in key positions are accountable for preserving ICT resources, everyone who purchases, uses or managers ICT

resources must bare some responsibility to ensure that integrity, availability and confidentiality of information are not comprised.

- All organizational information is considered valuable and sensitive to some degree. By identifying an organization's IT resources as having some level of value and sensitivity, it follows that all information requires security consideration.

For implementation of an information security program, the organization's information security program should be broken down into specific stages as follows:-

- Adoption of a security policy.
- Security risk analysis.
- Development and implementation of security standards and manuals.
- Development and implementation of the information classification system.
- Development and implementation of security self-assessment process.
- Maintain an on-going security program and its enforcement.
- Maintain an ICT cum security issue driven training.

The security policy should capture physical and operational security. Among the elements to be included in this part are:

- Site design
- Physical access
- Fire protection.
- Environmental protection of protected systems e.g. protection against floods, control of temperature and humidity.

Another component worthy being factored in security policy is information management. This should capture the following:

- Systems administration.
- Sensitive information control.
- Sensitive information security.
- Third party access.
- Prevention of computer misuse.

Systems integrity and security measures are also crucial and should be included in the ICT policy for the organization. The elements here include:

- Use of security systems or facilities.
- Systems access control.
- Password management.
- Privileged users management.
- User account management.
- Data and resource protection.

The policy should also have provisions for sensitive systems protection. Data center operation security stipulations are also important. They comprise:

- Job scheduling
- Systems operations procedure
- Medium management.

Back-up and off site retention should also be included in IT security policy. Up-to-date backups of all critical items should provide for minimum essential level of service. They include:

- Data files.
- Utility programs
- Databases
- Operating systems software
- Application system software
- Encryption keys.

The policy should make a provision for trails, audit and verification. Issues to be monitored include:

- Transactions
- Who, when, where, what and why accessed system.
- Significant security events: time, volume, frequency and type of information accessed.
- Time clock of computer systems to ensure accuracy of audit logs.

The policy should factor in measures to handle viruses. Among the measures are:

- Files servers and personal computers being installed with up-to-date virus detection and protection software.
- The detection software should be used from time to time to scan storage media and other renewable media to check for viruses.
- Put in place procedure to deter spread of viruses to other organizations e.g. communicating with or warning of other business partners who may be susceptible to virus attacks, setting up of procedures for documenting, communicating virus incidents, eradication and recovery. Users should also be trained on virus protection and controls.

The following are also worthy being part of security policy whenever a computer and its peripherals are relocated for maintenance, re-installation, re-configuration or storage purposes.

- Removable media should be kept in a secure location.
- Internal drives should be overwritten, reformatted or removed.
- Paper and ribbons should be removed from printers and destroyed or safely kept.

Since maintenance is a crucial factor about the performance of hardware and software, the following should be considered for the policy.

- ICT equipment should be well located / installed to protect them from electromagnetic interference.
- Changes to hardware and security features must be authorized and documented.
- Maintenance engineers for sensitive systems must sign a non-disclosure agreement before being contracted. Where maintenance takes place, authorized personnel should supervisor the exercise.
- After a maintenance exercise, all security parameters should be modified or changed to eliminate potential security exposure. Thereafter the system must be scanned for virus before being used.

For ICT security to be achieved, there must be provision for network administration within the ICT security policy.

- Organizations should designate properly trained network administrators who will be responsible for operation, monitoring security and functioning of the network.
- Network administrators should regularly undertake the review of the network and also provide physical, logical and procedural safeguards for its security.

- The computer security system should include a mechanism for alerting the network administrator of possible breaches in security such as unauthorized access, virus infiltration and hacking.

On security of network communication, the policy should provide for the following:

- All sensitive information on the network should be protected by using appropriate techniques. Network devices such as routers, switches and modems should be protected from physical damage.
- The network configuration and inventories should be documented and well maintained. Prior authority from the network administrator should be sort before making any changes to the network configuration.
- There should be an on going review of threats and network risks after changes in the network configuration.
- The network should be monitored for security irregularities and if identified, be addressed through a formal procedure.
- Physical access to communication and network sites should be controlled and restricted to authorized personnel as earlier on suggested.

There must be a provision for connectivity in the policy. Among pertinent connectivity concerns are:

- Procedures for allowing connectivity for computer networks to other networks outside the organization should be established.
- Permission to connect to other computer networks should be approved by the network administrator.

- Unused connections and network segments should be disconnected from the active network.
- Personal computers or outside computer system/terminals accessing an organizations host computer should adhere to system security and access control guidelines.
- There should be no internet access to data base servers, file servers or servers hosting sensitive information.
- The level of protection for communication and network resources should be commensurate with the criticality or sensitivity of the data transmitted.

In all human activities, emergency preparedness is crucial, so to a computer environment in which, emergency response for all activities related to computer operations should be developed and documented. Emergency drills should also be held periodically to ensure that the documented emergency procedures are effective.

Closely related to the above is disaster recovery and management preparedness. To achieve this, disaster recovery plan should be developed, be properly documented, tested and maintained to ensure that in the event of a failure of the information system or destruction of the computer facility, essential level of service will still be provided. The disaster recovery framework should thus comprise:

- Emergency procedures describing the immediate action to be taken in case of a major incident.
- Fall back procedure or alternative plan describing the actions to relocate essential activities or support services to a back-up site.

- Restoration procedures describing the actions to be taken to return to normal operations at the original site.

Finally, an ICT security policy must have space for contingency recovery equipment and services:

- Commitment should be obtained in writing from computer equipment and supply vendors to replace critical equipment and supplies within a specified period of time following destruction of a computing facility.
- The need for back-up hard ware and other peripherals should be evaluated depending on the business needs.
- A business continuity plan should be developed which should include the procedures for emergency, ordering of the equipment and availability of services.

In a nutshell, security domain includes confidentiality, availability and integrity. Thus, just protecting information from unauthorized access is not enough, it is equally important to ensure that electronic information remains accurate, complete and authentic (integrity) and can be used when needed (availability). Security policy must stress a combination of security organization and administration, physical security (use of physical barriers, logs etc), information technology security and personnel screening to determine their reliability and loyalty to the organization they serve. Above all, organizations should determine the security needs (risk management approach to security) for information and assets under the control by assessing the relevant rates and risks.

5.42 CONCLUSION

It has emerged from the study that some organizations in Nairobi have, on average, established electronic security systems to prevent unauthorized access to information. This is because certain information in the organizations is only viewed by certain officers. Since some information or record titles may reveal sensitive information, they are protected from unnecessary access. Restricting access thus provides good security.

Further, a good electronic information system provides multi dimensional functional security to reflect the need of the individual users. As such every organization has users with different requirements from an information system and in order to maintain some quality and consistence in an information database, access to update functions is restricted. Finally, a good electronic information system should provide both physical and logical access security. Thus only a limited number of staff needs to be involved in preparation or revision of information file, and access to information must be on need to know basis.

In conclusion, as we appreciate the value of information by the government and the organizations under study, threats against that information and the risks of information being realized, the place of security in any discussion of electronic information seems essential. The challenge to the government and the organizations studied is therefore of rethinking their laws/rules/regulations viz a viz security of information in the cyber space era, so that they maximize the driving forces propelling them to exploit the full potential

benefits of Information Society, while at the same time minimizing the negative constraining forces acting as barriers to frustrate this exploitation.

5.43 RECOMMENDATIONS

In view of the findings and conclusions discussed in this chapter, the following recommendations are made: The recommendations made here for electronic information security improvement are not exhaustive, however, they provide a way forward to securing electronic resources. They are derived from the several measures suggested by respondents and from the literature reviewed.

Recommendations for logical/systems security

- Just as Mutonyi (2003) suggests, foremost, a risk analysis, need to be undertaken to determine assets that require security, the likely dangers that they must be protected from and the best method of securing them.

- An electronic information security policy should be developed. The policy should be issue driven and consistent with other organizational policies.
- There should be regular updating and upgrading of hardware and software to address obsolescence. Data should be emulated and or migrated to other storage media compatible with the prevailing technological trends. There is need for use of virtual computers, which can take instructions from current and even future computers.

- To counter unauthorized access, interception and other logical threats, enhanced use of passwords, user IDs, administration rights and encryption are highly recommended. Information back up is emphasized by many specialists as the best fall back position in case of the original being interfered with.
- Electronic information should be kept as much confidential as possible. Confidentiality involves preserving the integrity of the data and user details; for instance, no units of data blocks received should be altered.
- Information resources should be classified and labeled according to sensitivity and importance of information transmitted. Storage media such as floppy diskettes, magnetic tapes, removable hard disks, optical disks etc. should be secured according to the classification of the information they store.
- Electronic communication systems such as network devices and computers should be equipped with suitable security software and if necessary with encryption and decryption software.
- Damaged media or information should be well disposed off to avoid opportunists making capital out of them.
- Removable electronic media must be removed from the computer and be properly secured at the end of the work session.
- Hard disks containing sensitive information should be securely erased prior to giving the information system to another department for maintenance. It is recommended also that maintenance should be internally undertaken and should be restricted to a particular engineer of a particular firm for accountability.

- To fight the virus menace, the sampled population suggested the use of in built anti virus software such as threats tracer application suggested by the Symantec (ICT vendor) respondents. Included here is the fire walling of the systems and sites and installation of self deleting software among others. All these examples of antivirus software scan, identify and repulse or destroy (delete) any system bound virus to ensure safety of information. Such software should undergo continuous upgrading to counter newly created viruses and should be installed in a centralized server, which work as the hard disk for other workstations. In addition, use of foreign diskettes must be avoided. If they must be used, they must then be first scanned for viruses. Finally, opening mails or attachments before scanning them for viruses must be avoided.
- To steer clear of computer errors and accidents, the following control measures are recommended.
  (a) Give various file access privileges and roles to the end users and technical staff in the organization, thus deny access permissions to certain groups of users for certain files and computers.
  (b) Set up a comprehensive error recovery strategy in the organization.
- To deter software piracy, the following should be done:
  (a) Enact laws that protect the owners of data and information against piracy.
  (b) Make software cheap enough to increase affordability and use licenses and certificates to identify originals
  (c) Set installation passwords that deter illegal installation of software.

5.44 Recommendations for physical security

Computer infrastructure, organization standards, operating procedures and personal information should be physically secured. The following are a must do for all organizations using information communication technology in Nairobi.

- Information communication centres or rooms should always be on upper floors to protect them from floods. Such rooms should be water tap free to avoid incidents of water running due to sheer carelessness or accidental leaving water tab(s) on.
- Computers and their related accessories should be placed in a controlled access and secure room or building, which should be strictly out of bounds for unauthorized persons.
- Computer sites should be located in secure environment devoid of fire and chemical contamination or explosions. The site should be constructed with fire resistant materials that are free from toxic chemicals.
- Computer room walls should be of sufficient thickness to resist forcible attacks. The doors should be burglar proof and windows facilitated with sturdy grills and or impact resistant laminated security glass and burglar alarms.
- Mission critical facilities such as servers should be designed for reparability, relocation and reconfiguration. Where possible, backups for mission critical facilities should be in remote places where access is granted only to specific authorized individuals on a need basis.
- There should be a 24-hour round the clock surveillance by authorized persons to provide physical security to the building and information technology equipment.

- A biometric physical access security system should be installed at all high security installations to control and audit access to the operational site.
- There should be a maintained up to date list of persons who access the ICT rooms. Besides, an inventory for and/or issue of access keys or cards should be put in place and all individuals visiting the computer centers should sign in and out, and must be accompanied by ICT staff at all times.
- Due to lack of a known full proof security, necessary precaution must be employed to deter attackers. As such the most trusted people should be given the responsibility of being in charge of the overall security of the organization.
- Access to information should be on a need to know basis. Users should only be matched with the information they have been cleared to work with.
- Organizations should set up procedures to authenticate information users.
- Organizations should install trip wires to set off alarm as soon as an unauthorized activity is detected.
- There is need for a comprehensive overhaul of framework of legislation to address specific threats to electronic activity and infrastructure. This will preempt the rise of cyber crime in its most nascent stages and also act in concert with the global community to combat cyber-crime. Such a legislative structure which captures emerging ethical notions that delineate minimum rights and liabilities of internet users can lay the juridical foundation for a predisposition of IT driven National developments.
- Among some issues to be captured in the legal framework of ICT include:

  (i) Access and transfer of data or information must be by owners' permission.

(ii) Data and information must be secured against loss or exposure to maintain confidentiality and integrity.

(iii) ICT information should be collected, kept and used for lawful or agreed purposes.

- To protect sensitive systems such as those dealing with financial transactions, security tokens or smart cards and biometric technologies such as iris recognition, finger print verification etc should be used to complement the usage of password to access the computer system. Further, access by other organizations should be prohibited or strictly controlled for computer systems processing sensitive data. As already pointed out, encryption of sensitive data and storage should be used to protect data and systems integrity and confidentiality.

To sum up, the ICT specialists, users and vendors seems to strongly suggest the use of backups, passwords and ID numbers to secure information. They are also agreed on the scanning of foreign diskettes to determine their suitability. At most, it emerges that foreign diskettes should completely be discouraged. Antivirus software and in-built firewalls are highly recommended to fight the virus menace.

For successful installation of ICT security hardware and software gadgets, it is recommended that the cost of ICT equipment be reduced. This can be realized if the government zero-rated taxes on the ICT equipment. Organizations should also set aside enough funds to go about achieving full proof security. Such monies become handy for equipping personnel with the relevant security skills and also in putting up state of the art

secure ICT rooms or facilities. Last but not the least, the government should not only develop an ICT security policy but also put it into practice by enacting laws, which executes and protects the policy. Finally, as already hinted, this research is not exhaustive about issues concerning security of electronic information in organizations in Nairobi. Besides, there are other many organizations in the country that deal with information communication technology. Against this backdrop, I recommend that further studies be done on security of electronic information in the rest of the country in view of the ever-changing technology and the ever-innovative cyber criminals who seems to hold ICT users and or information consumers to ransom. Once all these recommendations are adhered to, there is no doubt that information communication technologies and the information transmitted thereof will enjoy some security.

5.45 REFERENCES AND BIBLIOGRAPHY

Associated Press Hackers attacks warning issued. *East African Standard*, July 4. 2003 . Nairobi.

Associated Press. (2003). Hackers plan mass attacks. Saturday Nation, July 5th, 2003. Nairobi.

British Broadcasting Corporation. (2003). Science in Action. East African Standard. July 4th, 2003. Nairobi.

Daily Nation, (January 22nd, 2003). Digital Dark Age approaches.

Gerald, K.L. (2000.9). Managing an information protection program. Butterworth, U.S.A.

Government of Kenya. (2003.16). Electronic communications and electronic transactions Act, 2003. Nairobi.

Government of Kenya.(2003.34). Government Information and Communications Technology (ICT) policy. Nairobi.

Government of Kenya (2004.29). Information and Communication Technology (ICT) policy draft. Unpublished. Nairobi.

Hey W. (1997.275). Securing Windows NT. *PC Plus*. Issue 133.

I.R.M.T. (1999.28). Managing Electronic Records. International Records Management Trust. London.

Kovasich, L.G. (1998.ix) Information security officers' guide: Establishing and managing an information protection program. Burtterworth. Heinneman, USA.

Manoff, M. (2000.857). Hybridity, Mitability, Multiplicity. Theorizing electronic library collections. *Library Trends.* Vol. 49, No. 1.

Microsoft Corporation. (2003.5). Security advisory

Miller, R.H. (2000.645). Electronic resources and academic libraries, 1980-2000: *A historical perspective. Library Trends*. Vol. 48, No. 4.

Ministry of Finance, (2003.6). Environmental protection of data. *A paper presented to the National information and communication technology conference, held at the Kenya school of Monetary studies, 23-28th March.*

Mugenda, O. (1999.190) Research methods: Quantitative and Qualitative Approaches. Nairobi. ACTS Press.

Mutonyi, K. (2003.16). Information preservation: Challenges in the 21st century Globalization and security. *A paper presented during the regional conference on Information preservation held on 20th-21st March 2003.*

National Aeronautics and Space Agency (NASA). (2000.231). *NASA Procedures and Guidelines. Security of Information Technology. NASA.* 231. U.S.A.

Ngugi (2005.7) Law on cyber crime. *An article published in the Daily Nation, February 7th, 2005.*

Onunga, J. (1998.193). The Internet. University of Nairobi. Information Systems Academy. Nairobi.

PC Plus (1997-8). Anti spam measures. Future Publishing. United Kingdom.

Purser M. (1993.123). Secure Data Networking. Artech House, Boston, London.

Schweizer, D. (2002.216a). Securing the network from malicious code: *A complete guide to defending against viruses, worms and Trojans*. Wiley Publishing, Indianapolis.

Saturday Nation, (March 1st, 2003.1). How Euro debtors files were destroyed. Nairobi.

Sherman, K (1998.302). Data Communications. A user's guide. Prentice Hall Company. Virginia.

Steve. W. (2001.98). e Business essentials; technology and network equipments for mobile and online markets. England. John Widely and sons.

Stoll, C. (1989.22). Tracking a spy through the maze of computer espionage. New York; Doubleday.

Symantec operation. (2004.12) available at www.symantec.com/uk/small business/

Tennant, R (1999.30). Time is on our side: The challenge of preserving digital materials. Library journal, 124 (5).

Thomas, J. (1998.41). Spam wars. *PC Plus*. Issue 136.

William, J. (2004.249). All the Software you need to liven up your on-line presence. Prentice Hall. USA.

Zandonella C. (2002.44). *For the love of machines. New Scientist*. U.S.A

Internet sources.

http://www.mcrosoft.com

http:/www.Symantec.com/uk/small business. A symantec operation, 2004.

http://www.microsoft.com/piracy/basics/what/Africa/licencing

http://www.microsoft.com/piracy/basics/what/ip.asp

http://www.microsoft.com/security/defaul.asp.

http:www.virusbtn/

Appendix 1

Ben W. Namande
Kenyatta University
Library Studies Department
P.O.Box 43844
NAIROBI
3/5/04

Dear Sir/Madam,

RE: DATA COLLECTION MISSION FOR A MASTERS DISSERTATION.

As a partial fulfillment of the requirements for a Master of Education in Library and Information Science, Kenyatta University, I, the undersigned wish to request you to fill the questionnaire here attached. The purpose is to make an assessment of security of electronic information in selected organizations in Nairobi and thereafter make recommendations for security improvement in the organization studied.

Any information you provide will be treated with utmost confidentiality and used only in the realization of the objective outlined above. Thank you.

Yours faithfully,

Ben Wekalao Namande
E/55/7860/03

Appendix 2: QUESTIONNAIRE SCHEDULE FOR IT SPECIALISTS AND OTHER STAFF

TOPIC: Assessment of security measures for electronic information in selected organizations in Nairobi.
Instructions : Where multiple choice answers are provided ,use a tick for your answer and where not, answer as instructed.

1. Respondent's bio data.

Name (Optional):.....

Age.....Between 19 and 25 years [ ]
Above 25 years [ ]

Sex.....Male [ ]
Female [ ]

Nationality.....
Occupation.....
Designation.....Librarian [ ]
Systems Administrator [ ]
IT specialist [ ]
Telephone operator]]
Bank teller [ ]

Any other , please specify.....

Position.....Senior management [ ]
Middle management [ ]
Any other, please
specify.....

Responsibilities.....
.....
.....
.....
.....
.....

2. Background information about the organization

Name of the organization (optional).....

Category of organization.....Public [ ]

Private [ ]

Type of organization.....Financial [ ]

Information center//Library [ ]

Academic/Training [ ]

Research [ ]

Communication institution [ ]

Any other, please specify.....

.....

Year of establishment.....

Purpose and core functions of the organization.....

.....

.....

.....

Is there any statutory policy document e.g. parliamentary act ,regulating the organization's activities ?

If yes, briefly state the policy.....

.....

.....

.....

.....

.....

.....

.....

Is your organization attached or affiliated to any organizations, both locally and internationally?

If yes ,which ones?

a) Locally.....

.....

.....

.....

.....

(b)Internationally.....
.....
.....
.....
.....

3. Specifics on electronic facilities.

(a) Do you make use of information as an individual or as an organization? If yes ,which of the following facilities are used in your organization?

Computers	[ ]
Fax machines	[ ]
Telephones	[ ]
ATM's	[ ]
CD's	[ ]
Floppy disks	[ ]
Cartridges	[ ]
Video tapes	[ ]
DVD's	[ ]
Scanners	[ ]
Microfilms	[ ]
Satellites	[ ]

Others, please specicify.....
.....
.....
.....
.....
.....

(b) How are the above facilities utilized in your organization?
Incase of :

(i) Computers	Archiving purpose	[ ]
	Updating client's data	[ ]
	Data computation	[ ]
	General office work	[ ]
	E-services eg. E-mail, E-commerce, etc	

Others,
specify.....
.....
.....

(c) Telephone/Telex/Fax
Official use [ ]
Private use [ ]
Commercial use [ ]
Any other,
specify.....
.....
.....
.....
.....

4 (a) Do you have a policy, whether formal or informal that regulates acquisition ,use and maintenance of electronic information and or telecommunication equipment?.....

(b) If yes ,why was the policy developed?.....
.....
.....
.....
.....
.....
.....

(c) When was the policy developed?.....
.....

(d) Does the policy capture the element of security of electronic equipment and the data/information transmitted therin?.....
.....

(e) If yes ,why was the security element included?.....
.....
.....
.....

.....
.....
.....

(e) What aspects of security are covered within the security component?.....
.....
.....
.....
.....
.....
.....

5. For each of the electronic facilities stated in No.3,what security measures have you put in place to safe guard them against:

(a) Internal threats?.....
.....
.....
.....
.....
.....
.....
.....

(b) External threats?.....
.....
.....
.....
.....
.....
.....

(c) How do you ensure and maintain the confidentiality of the by-products of the facilities e.g.
Payrolls, print outs ,messages ,etc?.....

.....
.....
.....
.....
.....
.....
.....
.....
.....

(d) In the case of telephones and their accessories, fax telex etc how do you protect information from

(i) Eavesdroppers?.....
.....
.....
.....
.....

(ii) Masquerades?.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

(iii) Interception

.....
.....
.....

(iv) Dubbing?.....
.....
.....
.....
.....
.....

.....
.....

(e) During information/data transmission circulation, dissemination, and or communication, what security measures do you employ to ensure that the information is used for intended purposes and not any other activity?.....
.....
.....
.....

(f) Incase your organization uses ATM's credit and other related electronic cards, how do you protect:

(i) Users from fraud?.....
.....
.....
.....
.....
.....
.....
.....

(ii) Client's rights to privacy?.....
.....
.....
.....
.....
.....
.....
.....

(iii) How do you ensure that there is no unauthorized access and or withdrawal of clients cash from within or without your organization?.....
.....
.....
.....
.....
.....

(iv) In case of electronic money transfer from one organization or one point to another, what measures do you put in place

to ensure that the cash reaches the intended destination and recipient
safely?.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

6. Physical media security

(a) How have you physically secured your computer hard and software plus data thereof against malicious destruction like what happened in Euro Bank?.....
.....
.....
.....
.....
.....
.....

(b) What safety measures have you put in place for the hardware, software and other electronic information storage media such as CD's, DVD's etc, against deterioration from:

(i) Environmental
Conditions?.....
.....
.....
.....
.....
.....

.....
.....
.....
.....

(ii) Physical damage due to heavy usage or poor handling?.....
.....
.....
.....
.....
.....
.....

(iii) Technological obsolescence?
.....
.....
.....
.....
.....
.....
.....

(iv) Vandalism.....
.....
.....
.....
.....
.....
.....
.....

(v) Floods.....
.....
.....
.....
.....
.....
.....
.....

(vi) Fire.....
.....
.....
.....

.....
.....
.....

(vii) Wars and terrorism.....
.....
.....
.....
.....
.....
.....

(viii) Other perils (please specify).....
.....
.....
.....
.....
.....
.....
.....

7. Does your organization have a disaster preparedness, management and recovery plan?.....

If yes state briefly what it entails.....
.....
.....
.....
.....
.....
.....

8. (i) Does your organization charge for services that are offered?.....

If yes, which of the following means do you use for costing?

(a) Value [ ]
(b) Quality of information [ ]
© Time taken to access information [ ]

(d) Purpose e.g. research, commercial etc [ ]

(ii) How do you rank your security measures?
(a) Very effective [ ]
(b) Effective [ ]
© Fairly effective [ ]
(d) Not effective [ ]

(iii) In your opinion, are there other problems associated with the security of electronic information? Yes/No

If yes, state
them.....
.....
.....
.....
.....
.....
.....
.....
.....
(iv) Make suggestions and or recommendations to address the above and any other security problems in your organization's electronic information systems.....
.....
.....
.....
.....
.....
.....
.....

Thank you for completing this questionnaire.

Appendix 3: QUESTIONNAIRE FOR ELECTRONIC INFORMATION USERS /CLIENTS

INSTRUCTIONS

1. Tick appropriately in the square brackets provided or fill in the spaces provided.
2. Feel free to give any other relevant information not covered in this questionnaire on a separate sheet of paper.

A. GENERAL USERS BIO-DATA AND ORGANIZATIONAL INFORMATION

1. Name(optional).....
2. Sex.....Female [ ]
   Male [ ]
3. Nationality.....
4. Age Below 14 years [ ]
   Between 15 and 25 years [ ]
   Over 25 years [ ]
5. Occupation.....
6. Category of organization used.....Public [ ]
   Private [ ]
7. Type of organization used Financial [ ]
   Information center/Library [ ]
   Academic/training [ ]
   Research [ ]
   Communication organization [ ]
   Any other, specify.....

B. ACCESSIBILITY AND SERVICES USED

1. What organizations do you interact with in the area of electronic information and user service utilization?

Information centers [ ]
Telecommunications [ ]
Banks [ ]

Cyber cafes [ ]
Any other,please
specify.....
.....

2. How did you come to know about the existence of the organization you use as indicated above?

Through the media(print and electronic) [ ]
Through colleagues/friends [ ]
By chance [ ]
Any other, please
specify.....

3. How do you utilize or to what use do you put electronic information services?

Surfing the internet for research purpose [ ]
E-mail service [ ]
Making telephone calls [ ]
Goods purchasing [ ]
Banking services e.g. banking and withdrawal of cash [ ]
]
Any other, please
specify.....
.....

4. (i) What kind of information communication technology/facility do you use in the organization(s) you indicated in question 1?

Computers [ ]
Telephone, mobile and landlines [ ]
ATM services [ ]
CD's [ ]
DVD's [ ]
Floppy disks [ ]
Scanners [ ]
Others please
specify.....
.....
.....
.....
.....

(ii) Are these ICTS physically secured ? Yes/No. Explain your answer.....

.....

.....

.....

.....

.....

5. Do you experience any problems when utilizing information communication technology? Yes/No

If yes , state the problems experienced.....

....

.....

.....

.....

.....

.....

6. Have you experienced any security problems or limitations when utilizing information communication technology? Yes/No.

If yes , which among the following?

Hacking [ ]
Information leakage [ ]
Eavesdropping [ ]
Loss of information [ ]
Alteration of information [ ]
Hardware damage [ ]

Any other, please specify.....

.....

.....

.....

.....

In your opinion ,are the security measures in place, e.g. use of PIN, a hinderance to information access? Yes/No.

Explain your answer.....

.....

.....

.....

.....
.....
.....

7. In your interaction with the ICT at your user station, are you assisted by the organizations staff? Yes/No.

If yes, under what
circumstances?.....
.....
.....
.....
.....

9. Are staff equipped with necessary skills and experience to ensure security of the electronic systems? Yes/No.
For your answer above how do you rate their experience?
Below average [ ]
Average [ ]
Above average [ ]

.....

8. Give any recommendations and suggestions on how to avoid security problems being experienced.

.....
.....
.....
.....
.....
.....

Thank you for having responded positively by answering this questionnaire.

Appendix 4: QUESTIONNAIRE FOR I. C.T DEALERS AND /OR VENDORS

INSTRUCTIONS

1. Tick appropriately in the square brackets provided or fill in the spaces provided.
2. feel free to give any other relevant information not covered in this questionnaire on a separate page.

A. GENERAL INFORMATION AND RESPONDENT'S BIO-DATA

1.Name (optional).....

Sex Female [ ]
Male [ ]

Age Between 19 and 25 years [ ]
Over 25 years [ ]

Occupation.....

Responsibilities.....

B. BACKGROUND INFORMATION ABOUT THE ORGANIZATION

2. Name of organization (optional).....

Year of establishment.....
Objectives of organization.....

3. Is there any policy regulating the organization's operations? Yes/No

If yes, state the policy.....

4. Is your organization attached or affiliated to any other organizations both locally and internationally? If yes, which ones?
   (a) Locally.....
   (b) Internationally.....

C. SERVICES

5. What kind of ICTs do you deal with?

6. (a) Is the component of information security captured in your ICT's and s it available to clients on request? Yes/No.

   (b) If yes, what aspects are covered under information security as regards:
   (i) Physical security.....
   (ii) Systems security.....

7. Generally speaking, electronic information and its accessories are prone to several (in) security related dangers.

   What measures have you put in place to guard against the said dangers?.....
   .....

Thank you for sparing time off your schedule to fill my questionnaire.