AN INVESTIGATION ON DISASTER PREPAREDNESS AND MITIGATION FOR COMPUTER BASED INFORMATION SYSTEMS IN SELECTED UNIVERSITY LIBRARIES IN KENYA

BY

ROSE WAMBUI NJOROGE

E83/13265/2009

A THESIS SUBMITTED IN FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY IN THE SCHOOL OF EDUCATION OF KENYATTA UNIVERSITY

SEPTEMBER, 2014

DECLARATION

This thesis is my original work and has not been presented for any award of a degree in any other university. Reproduction of any part of this thesis should not be done without permission from the author and /or KENYATTA UNIVERSITY.

_____ _____

Signature **DATE**

ROSE WAMBUI NJOROGE
Department of Library and Information Science
Kenyatta University

We confirm that this thesis has been submitted for examination with our approval as University Supervisors.

_____ _____

Signature **DATE**

DR. DANIEL W. MUTHEE
Department of Library and Information Science
Kenyatta University

_____ _____

Signature **DATE**

DR. NORBERT. OGETA
Department of Educational Management, Policy and Curriculum Studies
Kenyatta University

DEDICATION

I dedicate this work to our three little “angels” Anthony, Michael and Gabriel who did not understand why mum was absent most of the times during the course of my study and kept on urging me to finish my “homework; to my late mother, Margaret Wamuyu, I know you always wished me well.

ACKNOWLEDGEMENTS

To accomplish this task, many people went out of their way to ensure the journey was smooth. It was my wish to mention all of them, but since it is not possible, I wish to acknowledge a few of them, although my thanks go to all of them.

First, I wish to thank the Almighty God for His Grace which saw me through the whole journey of this programme. I thank my supervisors, Dr. Daniel W. Muthee and Dr. Norbert Ogeta, most sincerely for the advice, direction and encouragement. Heartfelt gratitude goes to my employer, Kenyatta University, for the financial support and time to undertake this study. Gratitude to my colleagues in the Department of Library and Information Science for the support and encouragement. Dr. Kisa Amateshe deserves appreciation for editing the final work.

To my husband and friend, Dr. Francis Njoroge, for continuously reading my work and his insight contributions, I register my gratitude. Many thanks to our children: Anthony, Michael and Gabriel, for being so patient and understanding and always urging me to finish my "homework" before asking me to take them for an outing. To my family members for their constant emotional and material support and to any person who contributed to this thesis in one way or another, I thank you all.

TABLE OF CONTENTS

LIST OF TABLES

Table **Page**

LIST OF FIGURES

Figure **Page**

LIST OF PLATES

Plate **Page**

ABBREVIATIONS AND ACRONYMS

BIOS:	Boot Input Output System
BIRA:	Business Impact Response Analysis
CBIS:	Computer-Based Information Systems
CBLIS:	Computer-Based Library Information Systems
CCTVs:	Closed Circuit Televisions
CD:	Compact Disk
CD ROM:	Compact Disk Read Only Memory
CL:	Circulation Librarian
CPU:	Central Processing Unit
DCP:	Disaster Recovery Planning
DCP:	Disaster Control Planning
DM:	Disaster Management
DMP:	Disaster Management Plans
DR:	Disaster Recovery
DRP:	Disaster Recovery Plans
DUL:	Deputy University Librarian
DVD:	Digital Versatile Disk
ICT:	Information and Communication Technology
ICTD:	Information and Communication Technology Director

ICTDT:	Information and Communication Technology Director Technician
ICTT:	Information and Communication Technology Technician
IR:	Institutional Repository
ISL:	Information Systems Librarian
ISO:	International Standard Organisation
IT:	Information Technology
LMS:	Library Management System
OL:	One Librarian
OPAC:	Online Public Access Catalogue
PhD:	Doctor of Philosophy
RAM:	Random Access Memory
UL:	University Librarian
VCR:	Visual Control Recorder
VOiP:	Voice over Internet Protocol
WWW:	World Wide Web

ABSTRACT

This study was carried out at a time when the introduction of Information and Communication Technology (ICT) in higher institutions of learning had become a key issue for service delivery. The introduction of e-learning and hence the need to provide access to information for learning, teaching and research had necessitated academic libraries to incorporate Information Technology (IT) to facilitate efficient and effective operations of the library. IT has seen the introduction of computer-based information systems (CBIS) in the libraries. The study aimed to investigate the status of disaster preparedness and mitigation for CBIS in libraries. To achieve this, it sought to find out threats affecting CBIS, established disaster preparedness and mitigation measures, find out personnel involved in disaster preparedness and mitigation, assess policies and programmes on issues addressed on disaster preparedness and mitigation and finally the challenges faced by university libraries which may CBIS. The study was carried out in selected academic libraries in Kenya. These included two public and two chartered private universities within Nairobi County and its neighbouring counties (Kiambu, Machakos and Kajiado). The study respondents included university librarians, deputy university librarians, ICT directors, information systems librarians, ICT technicians working in the libraries and circulation librarians. A total of 26 participants were expected to participate in the study. However, only 19 were eventually interviewed. Relevant data was collected from the respondents using several methods which included observation, interviews, document reviews and audio-visual aids. The collected data was coded, analyzed, interpreted and presented using qualitative methods. This entailed coming up with themes, coding the themes and writing narratives for the findings and drawing conclusions. Data was presented using tables, graphs, charts and plates. The findings revealed that libraries had taken several measures to protect their CBIS. The researcher noted that only basic measures had been incorporated and the personnel in charge of CBIS had varied levels of training which influenced the methods used to secure CBIS. Top management of the institutions studied were not fully aware of the dangers CBIS were exposed to and relied heavily on the advice given to them by ICT personnel. Three of the institutions studied had not developed policies and programmes pertaining to disaster management for CBIS. There were a myriad of challenges experienced in a bid to mitigate and prepare for disaster that could affect CBIS such as vandalism, lack of cooperation by various departments, lack of funding, inadequate qualified staff to deal with CBIS, among many others. The study came up with several recommendations on education and training, disaster management policy development, training programmes and plans development, establishment of data recovery centres for CBIS, cooperation and partnership with other stakeholders, provision of adequate funding for CBIS infrastructure among many others. Further research was recommended on CBIS business continuity planning in universities in Kenya.

CHAPTER ONE

INTRODUCTION

1.1 Background to the Study

In the 1980s and 1990s, industries and institutions began to depend on automation to the fact that functioning manually had become nearly impossible for most businesses. Computer environments evolved into complex information infrastructures which led to proliferation of personal computer (PC) use, local area networks, distributed computing, client/server networks, the internet and the World Wide Web (WWW) (Kibaru, 2005). This made organizations to depend on the speed and efficiency of automated systems to deliver services to their customers. As early as 1992, many organizations became so dependent on computer-based and telecommunication-intensive information systems that disruptions of either caused outcomes ranging from inconveniences to catastrophe (Loch, Houston & Warkentin, 1992).

Preliminary investigation by the researcher about universities in Kenya showed that universities had introduced several programmes such as e-learning, distance education and part-time programmes as well as opened satellite campuses. This called for an effective and efficient access to information especially outside the institution. On the other hand, libraries had continued to automate their operations as well as offer services electronically. Some had established digital collections to ensure increased access to a wide range of information resources through the use of computers. Meckler (1991) notes that libraries in 1930-1960 marked the beginning of library automation where computers were used to automate library circulation and acquisition. He continues to note that the 1960s and 1970s

advances in the use of computers led to an explosion in library automation. Since then, libraries have increasingly continued to automate their major processes and services such as cataloguing, acquisition, catalogues, reference services, circulation of library materials, among others as reported by (Computer-Based National Information Systems: Technology and Public issues, 1981:8).

Wepman (2010) observes that computer-based information systems have been in widespread use since they provide fast and centralized access to databases, reference readings, among other benefits. He further notes that computer-based information networks are growing faster each year and libraries continue to rely on automation to get information from other departments within the institution through the Enterprise Resource Planning (ERP) software. Libraries thus rely on automation to reach the ever growing student population in the institutions and their satellite campuses. This enables them to get wealth of information from publishers through electronic databases for journals, e-books, and other electronic information resources.

Creation of Computer-Based Information Systems (CBIS) in libraries has been key in meeting the needs of library clients through effective and efficient access to information. Thus, disruption of these automated activities would be disastrous to the library operations and would greatly affect library clientele. It is, therefore, necessary to ensure that all resources are properly protected against possible threats given that the education environment has undergone a paradigm shift due to the rapid growth of technology as noted by Kritzinger (2006).

Increased use of information technology and reliance on computers by organizations redefine organisations' risks. The primary threat is to corporate data

due to unlimited access by a large, knowledgeable community of end users from desktop, dial-in, network facilities which create a new and extremely vulnerable environment (Loch et al., 1992). This means that the increased use of computer-based information systems (CBIS), leads to a tremendous increase of the threats that may affect these systems. Disaster management planning has, therefore, taken a new sense of urgency because of the expanding occurrence of various types of disasters associated with increased use of CBIS. Disaster planning becomes very important in managing a disaster as Kaur (2009) notes that lack of it can lead to immense loss when a disaster strikes.

The primary obligation of any academic library is to meet the information needs of its members (Feather and Sturges, 2003). To do this, libraries have introduced network services such as internet, electronic journal services; web Online Public Access Catalogue (OPAC), CD ROM searching services, and digital collections among others. This has become very important with the introduction of distance, open and e-learning programmes in institutions of higher learning. The introduction of these programmes calls for 24/7 access to information resources. The automated services help in providing equitable levels of service across the whole institution and to distant users. It is, therefore, important to ensure that these services are available whenever needed by clients. However, CBIS are prone to various kinds of man-made or natural threats or disruptions that may lead to a disaster.

Chow and Ha (2009) quoting Ginn (1989) identified top management commitment as one of the major factors for Disaster Recovery Planning (DRP) for information system functions in an organization. They further listed three

main reasons for protecting an organization's information systems and data, These are: budgetary allocation, DRP implementation as well as enhancing co-operation and support by various departments. Fitzgerald and Dennis (2002) point out that departments must be accountable for the control and security of an organization's computer network. Eden and Matthews (1997) emphasise that library IT personnel should liaise with internal computing department and service providers in establishing security requirements, temporary service and access arrangement at the time of disaster. IT personnel should, therefore, have knowledge relating to the organization's buildings, computing systems, equipment and electrical systems, among others.

Since disaster is inevitable, librarians ought to be prepared. The preparation against disaster will enable the library to recover quickly from it. This confirms the current motto for an insurance company in Kenya, "hope for the best, prepare for the worst". Organizations, therefore, need to prepare and mitigate for disaster of whatever nature. This can only be so if proper planning and preparedness are done before hand. Disaster preparedness and recovery planning should be in place since it is hard to prepare once a disaster has happened. Recovery is difficult if proper preparations had not been made before hand. It is, therefore, necessary to prepare for and prevent against what is preventable since this will minimize the dangers if and when disaster strikes. Safety of employees, facilities, equipment and information resource collections, the information systems in the library are all prone to all sorts of disasters. As the libraries need to prepare for disaster, it is worth noting that CBIS methods and procedures for disaster preparation and prevention may be quite different from those of printed or manual systems. CBIS are prone to other forms of disasters such as hackers, viruses, and intrusion that

may not be peculiar to the manual systems**.** At the same time, other factors such as dependence on telecommunication systems, availability of electricity and special cooling systems bring about other vulnerabilities unique to automated systems.

1.2 Statement of the Problem

University libraries have increasingly continued to automate in a bid to effectively and efficiently meet the information needs of their students, lecturers and researchers. A library, being the heart of any learning institution, is strategic in meeting its clients' learning, teaching and research objectives. With the introduction of open universities (distance and e-learning programmes, and part-time programmes as well as incorporation of digital collections in libraries), it is paramount to facilitate increased access to information. Computer-based library systems that support increased access must be safeguarded to ensure that they are functional, efficient and effective at all times. Cervone (2006) points out that disaster recovery planning and business continuity planning are two of the most critical components of the digital library system infrastructure, yet they are aspects that are often overlooked. The neglect of computer-based information systems is unfortunate because the consequences of being unprepared for disaster are significant. According to Cervone (2006), quoting Wheatman (2001), two out of five organizations that experience a disaster are out of business within five years. Libraries must ensure that disaster mitigation plans are in place so that their services and operations are protected from both preventable and natural disasters. Since it is hard to totally prevent disasters from happening, it is appropriate to ensure that plans are in place so that services and operations of the library are not adversely affected in case disaster strikes. At the same time, libraries should

ensure that there is continuity in service delivery even when a disaster strikes. This means that disaster mitigation plans should be comprehensive enough to cover preventive, preparedness, reaction and recovery procedures (Eden & Matthews, 1997).

Preliminary investigations by the researcher showed that many libraries had embraced ICTs for automating traditional library information systems and operations. The latter systems are vulnerable to threats such as flooding, earthquake and humidity but ICT systems come with their other peculiar threats that may cause disruptions or denial of service. Generally, studies on disaster management in libraries have concentrated on disasters affecting printed information resources and library buildings. Kaur (2009) looked at disaster planning for university libraries in India and dwelt on disasters that affect printed books and the library buildings. A survey on control planning for academic libraries in West Africa was carried out by Aziagola and Edet (2008) and concentrated on natural and man-made types of disasters. In Kenya, Wambiri (2008) studied disaster management for university libraries and concentrated on general disasters that could occur in a library. Kimani and Muthembwa (1998) also studied general disasters that occur in libraries and not those specific to library CBIS. Methods used to prevent and prepare for a disaster in a traditional library and its systems may be different from those used for CBIS. There exists a gap in knowledge on disaster management for CBIS in libraries in institutions of higher learning in Kenya. It is in this light that this study focused disaster mitigation and preparedness for CBIS in university libraries in Kenya. A quick search through the websites of universities in Kenya and websites of their

respective libraries indicated that all university libraries were automated. There was also evidence of electronic resources and electronic services to their clients.

University libraries have moved towards automation of their processes and procedures, and at the same time are offering services and have incorporated electronic information resources. Security of their computer-based information systems is paramount to ensure high availability of their services and operations, and to protect the huge investments in these systems. The study, therefore, sought to fill the existing knowledge gap on the controls that the university libraries in Kenya have put in place to prevent and prepare for a disaster; investigate what personnel are involved in disaster management for library CBIS; what policies and programmes are in place which address disaster preparedness and mitigation for library CBIS and the challenges that the libraries face in a bid to ensure security of their CBIS.

1.3 Purpose of the Study

The purpose of this study was to investigate the status of disaster preparedness and mitigation for computer-based information systems in selected university libraries in Kenya with an aim of filling the existing knowledge gap that exists in this area.

1.4 Objectives of the Study

The objectives of the study were to:

i. Find out what threats related to CBIS that the libraries experienced.

ii. Establish disaster preparedness and mitigation measures put in place by university libraries for their computer-based information systems.

iii. Find out what personnel were involved in disaster preparedness and mitigation for computer-based information systems in university libraries.

iv. Assess policies and programmes on issues addressing disaster preparedness and mitigation for computer-based information systems in university libraries.

v. Find out what challenges are faced by university libraries in a bid to prepare and mitigate for disasters related to their computer-based information systems.

1.5 Research Questions

The research questions for the study were:

i. What threats have the libraries experienced in relation to their CBIS?

ii. What measures have the university libraries in Kenya put in place to ensure security of their computer-based library information systems?

iii. Who are the personnel in-charge of disaster management in the institution and the library? What are their roles and responsibilities? What are their qualifications and education level?

iv. What policies, plans and programmes for disaster management are available in university libraries in Kenya? Do they exist? What issues do they address? Are they accessible?

v. What challenges do ICT department and university libraries face in their endeavor to secure the CBIS?

1.6. Assumptions of the Study

The assumptions of the study were:

i. The university libraries in Kenya have incorporated computer-based information systems in their day–to-day operations.

ii. The personnel charged with the responsibility of maintaining CBIS are aware of what CBIS and its security entails.

iii. University libraries in Kenya had not experienced major disasters for their computer-based information systems; as a result, they had not invested heavily in disaster management.

iv. Disaster management plans, programmes, and policies affected the methods and measures used for preparing and mitigating for disaster.

v. Institutional support, education, skills and equipment and budgetary allocation affected the development of disaster management policies and programmes for library computer-based information systems.

1.7 Significance of the Study

i. The study aimed to investigate the measures that university libraries in Kenya had put in place to prepare for and prevent disasters related to CBIS. This was to enable the researcher to have a better understanding of how CBIS were handled in university libraries.

ii. To provide university libraries with information on up-to-date methods and measures of securing the computer-based information systems.

iii. The study would sensitize university management and senior library staff on the need for disaster control planning for library computer-based information systems.

iv. The study findings could be used to make policy decisions on disaster management for CBIS by university management, government

stakeholders such as Commission for University Education, government ministries such as Ministry of Education, Science and Technology, Ministry of Information and Communication Technology, among others.

v. The findings from the study could be used by the university libraries to come up with policies and programmes that support disaster control planning of their computer-based information systems.

vi. The study findings could enable university libraries to offer effective and efficient services to their users regardless of their respective distances. This will be so by ensuring that the systems are protected from threats that could cause denial of service.

vii. The study is meant to be part of the basis for information and knowledge creation in the area of information science.

1.8 Delimitation of the Study

The study was limited to issues concerning disasters affecting library computer-based information systems and, therefore, did not deal with issues relating to disasters of library materials and buildings.

The study was limited to selected public and chartered private universities within and around the environs of Nairobi County. It was assumed that these had automated most of their library operations and services in order to remain relevant to their clientele. Public universities main libraries and not their constituent college libraries were considered for the study. It was assumed that the situation at the main library was a replication in the constituent library. The study was also limited to the fully-chartered private universities.

Only university librarians, deputy university librarians, information systems librarians (sometimes referred to as systems librarians), library ICT technicians and the University IT managers participated in the study. The study included these groups of participants because they are normally involved in decision making and implementation of ICT related infrastructures in libraries..

1.9 Limitations of the Study

The sensitive nature of computerized information systems meant that not all institutions were willing to give information in detail.

Since libraries were at different levels of automation, different methods were used to secure computer-based information systems depending on the size of the network.

1.10. Theoretical and Conceptual Framework

1.10.1. Theoretical Framework

Theories have four main purposes in scientific research which include: description, explanation, prediction, and control. A theory has been defined variously by different scholars. Zikmund (2003) defines a theory as a coherent set of general propositions used to explain the apparent relationships among certain observed phenomena which allow generalization beyond individual facts. Mugenda and Mugenda (1999) define a theory as a system that explains phenomena by stating constructs and the law that interrelates these constructs to each other.

According to Sekeran (2003), a theoretical framework is a conceptual model of how one theorizes or makes logical sense of the relationship among several factors that have been identified as important to the problem. But a model is a

description of phenomena that are abstracted from details of reality (Stockburger, 2004). According to Kebede (2002), models can be used to explain theories and are useful for specifying research focus and advancing theory in relation to the phenomena they model.

1.10.2 Integrated Disaster Management Model

An integrated disaster management model as seen by Manitoba Health (2002) is a means of organizing related activities to ensure their effective implementation. The model identifies four main components as follows:

i. Hazard assessment (identifying threats and vulnerabilities);
ii. Risk management (determining the implications and treatment options);
iii. Mitigation (eliminating or reducing the threats as possible and appropriate) and;
iv. Preparedness (developing and readying response and recovery actions).

These components are implemented as part of a strategic approach and each links quality improvement process which monitors and evaluates changes to the systems. All these elements are interdependent and each has its boundaries but they provide each other with critical support. An integrated disaster management framework encourages adoption of natural system approach. In this case, roles and responsibilities in case of a disaster reflect those undertaken in normal circumstances. The development of an independent 'disaster-only' system is prevented as this may conflict with the normal system. This is so especially in incidents where the nature or scale of the problem does not appear sufficient or consistent enough to trigger a ‘disaster’ response.

According to F/P/T Network for Emergency Preparedness and Response (2004):

> Natural system approach recognizes that ownership of disaster management planning must be linked to the day-to-day planning. In this way, the responsibility for disaster management permeates an organization. The value of an integrated disaster management framework is, it provides a coherent structure for how this responsibility is fulfilled within an organization.

A balance between flexibility and preparedness is provided by this model. The model acknowledges that disasters are unique events that involve a high degree of uncertainty. Thus, this requires a system that can respond fluidly to the specific demands. For the system to be adaptable and efficient, it must be based on pre-existing or pre-arranged activities. Using an integrated disaster management model, with its preference for natural systems allows for rapid change without needing drastic realignment of roles or responsibilities.

The model involves a cyclical process which starts with the strategic plan, identifies the functions and assigns responsibilities for various components. The initial task is hazard assessment that provides the information necessary for the risk management step. According to Manitoba Health (2000):

> This result in decisions on the balance of mitigation and preparedness actions needed to address the risks. All of these actions and their outcomes are evaluated through the quality improvement process that leads back to refining and maintaining the strategic overview of each component. In practice, there will be activities from all components occurring simultaneously. The whole model must be integrated into the management of the organization, whether the model is being applied by a facility, a department, or a sector. Different people and programmes contribute as information is generated, enhanced and shared at each step.

This model applies to this study since disaster preparedness and mitigation are core to reaction and recovery of a disaster. Also, the measures and controls employed include all the stakeholders where institutional and library management

are involved to ensure efficient and effective running of CBIS. Policies and programmes to guide disaster mitigation and preparedness ensure that the measures and controls have been put in place.

CONCEPTUAL FRAMEWORK

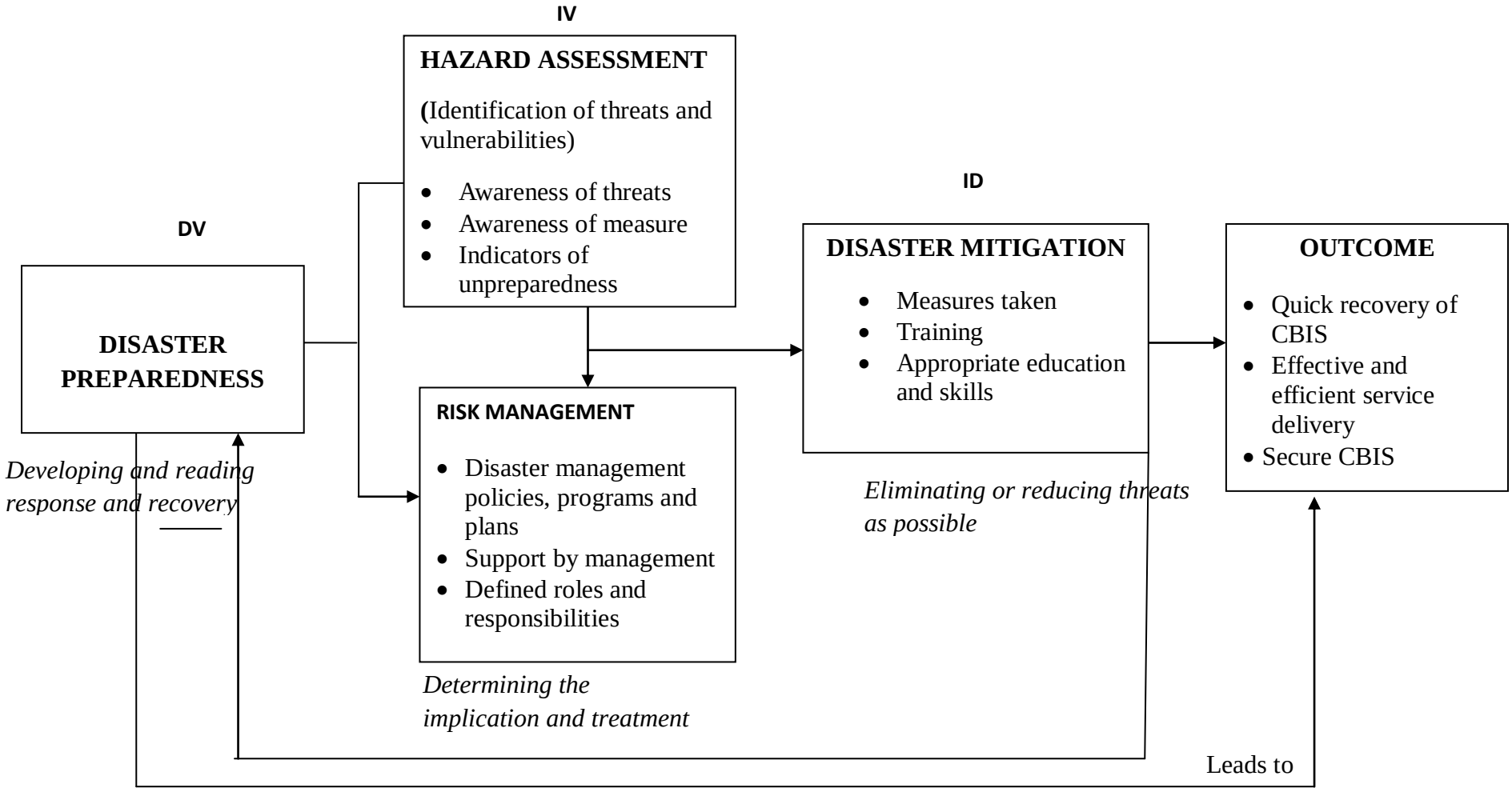

Figure 1: Conceptual framework; Disaster preparedness as a factor of disaster mitigation.

Source: Researcher's conceptualization from the integrated disaster management model

KEY
IV: Independent Variable
DV: Dependent Variable
IV: Intervening Variable

The conceptual framework shows that the goal of preparing for and mitigating against disaster is to ensure that if it happens, the librarians will be able to respond and quickly recover from its consequences. This can greatly be influenced by factors such as hazard assessment and risk management. When these two are done, the organization is able to eliminate or reduce threats that may cause disaster to CBIS. This leads to disaster preparedness and the outcome of this is quick recovery if and when a disaster strikes. This will also lead to effective and efficient service delivery as well as secure CBIS.

1.11 Operational Definition of Terms

Backup: A duplicate copy of data, files, documents, programmes that is normally taken and kept away from the original for security purposes in-case the original one is affected.

Circulation librarian: The person who heads the circulation services section/division in the library.

Computer-based Information Systems: Information systems where computers are used to automate the functions, services, procedures and operations of a library. This could either be a standalone computer or networked computer.

Disaster: Anything that causes disruption of CBIS system leading to lack of service.

Disaster management plan: Documented procedures or processes put in place to ensure smooth running of the IT system before, during and after a disruption.

Disaster mitigation: Measures taken to prevent disruption or failure of CBIS.

Disaster preparedness: Measures taken in readiness for a disaster.

Disaster prevention: Measures taken to ensure the IT systems are not disrupted or curb disaster from happening or to minimize disaster if it ever happens.

Disaster recovery: Measures taken to ensure IT system returns to normal after disruption, that is resumption of business to normal or almost normal if a disaster strikes.

Information system librarian: The person in charge of ICT related issues in the library.

Information technology manager: In some cases, the person is referred to as IT director. A person who oversees the ICT related issues in the University.

Library management: The senior library staff members who in most cases head sections or divisions in the library.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This Chapter reviews literature in line with the area of study. Bak (2004) indicates that literature review should have boundaries as it is not possible to review all there is in a subject. According to Oliver (2004), the principal purpose of literature review is to establish the academic and research area that is of relevance to the subject of the study. Khamadi (1992) defines literature review as an attempt to locate and synthesize completed research reports, articles, books and other materials on a specific research topic. Literature review is defined by Oso and Onen (2005) as a systematic identification, location and analysis of the documents containing information related to the research problem.

The literature reviewed in this study focuses on disasters that may occur in libraries, types or forms of disaster, disaster associated with computer-based information systems, prevention of disasters, disaster management plans, personnel in-charge of disaster management and their roles and responsibilities. In addition, the basic components of a disaster control plan; preventive, preparedness, reaction and recovery procedures are discussed.

To ensure that disaster management plans are written, implemented properly and kept up-to-date, it is very important to have related policies. The literature review explored policies, programmes and procedures that a library ought to put in place to ensure successful disaster management.

2.2 Types and Causes of Disasters

Shaluf (2007) classifies disasters into three main types: natural, man-made, and hybrid. Natural disasters are catastrophic events resulting from natural

causes such as volcanic eruptions, tornadoes, and earthquakes. Man has little control over these. Man-made disasters are those that result from human decisions. There are also disasters that result from both human error and natural forces which he refers to as hybrid disasters. Cervone (2006) groups disasters as technical threats such as power failure or computer hardware failure; natural threats such as floods, extreme winds, earthquakes, or volcanoes; and human threats such as error, extortion, burglary, chemical spills, explosion, vandalism, sabotage, or computer crime.

Several other authors group disasters into two main categories- Natural and man-made. (Kaur, 2009; Aziagba & Edet, 2008; Loch; Eden & Matthews, 1997; Kochtanek and Joseph (2004), describe the causes of disaster as power blowout or blackout, physical disaster; fire, floods, earthquakes, and security disaster; computer virus, hacking, and corruption of databases. McIntyre (1988) notes that a disaster can result from an act of vandalism. It could be fire resulting from arson, negligence or poor maintenance. In some regions of the world, there is a serious threat from earthquakes or extreme weather conditions such as hurricanes or tornadoes. Other causes of disaster identified include: flooding resulting from leaking roofs, water taps, drainage pipes, activities arising from mining, bomb explosions, wars, student unrest, fires, poor storage facilities, negligence, volcanic eruptions, fire and lightning.

Types and causes of disaster were addressed by various authors but they did not address the causes and types of disaster of CBIS in a library setting.

2.3. Library Computer-based Information Systems

By 1990, computer technology in libraries was seen as revolutionizing the concept of rapid and accurate information services (Khalid, 1999). Currently, computer-based information systems have been successfully introduced in all

types of libraries and information centres. With inception of computer technology in libraries, terms like “information technology”, “library automation”, and “information communications technology”, “computer-based information systems”, have become common in the library world. Computers, telecommunications, and micro electronics are used in libraries for obtaining, storing and transferring information. Khalid (1999) notes that the ability of a computer to carry out library functions quickly, accurately, and systematically makes it a most useful tool. This is because timely availability of information plays a fundamental role in the development of any organization in the country. Therefore, computerized services in libraries such as housekeeping routines, information storage and retrieval and networking become key to the delivery of efficient and effective services.

Today, computers are recommended for libraries because of their speed, accuracy and increased efficiency. Proliferation of information and the dissemination of information are made possible through the use of information communication technology. Computer-based library systems are developed and used to provide better services at a lower or insignificant cost, and to provide added economic benefits. In a public library, ICT becomes part of the nation’s modernization. Automation also enables libraries to place their entire collection at immediate disposal of their users. Once electronic systems are adopted, the number of activities also grow, the image of the library and that of librarians improves. Other benefits include: the flood of information, increased services to readers, efficiency and accuracy, resource sharing, flexibility, time saving, reduced amount of space taken up by print resources, simplicity, portability, durability and security of data, standardization and centralization of services.

The literature focuses on the use of computers in the libraries as well as benefits of automation in libraries. There is a gap on services and electronic resources that are offered through CBIS in libraries which this research hoped to fill.

2.4. Disaster and Computer-based Information Systems

2.4.1 Computer Disaster

Klein and Joseph (2007) observe that disasters can occur at various levels of intensity and that risks and uncertainties are part of the everyday operating environment for all organizations. If risks are left unattended, they can become a disaster. Crisis has been defined as an abnormal situation that presents extraordinary risks to a business and which may develop into a disaster unless carefully managed (Davies & Walters, 1998; Caelli et al., 1991).

Computer disasters may include: theft, virus, hacking, hardware faults, malicious damage, software problems, and environmental conditions such as humidity, human negligence and natural disasters (Loch et al., 1992). Other identified threats to information systems include: accidental entry of bad data by employee, intentional entry of bad data by employee, accidental and intentional destruction of data, unauthorized access to data system, inadequate control over media, hacking, computer viruses, inadequate physical control, natural disaster, fire, flood, loss of power, communication. Klein and Joseph (2007) add onto this list by including: hardware failure, malicious attacks via software, internet intrusions, and Mother Nature which can cause damage on computer systems. CBNI (2004) notes that threats against computer systems appear to be on the increase such as: theft, sabotage, data alteration, blackmail, system failure, service interruption, natural hazards, unauthorized disclosure and certain social conditions that may increase the threats to CBIS. Social

conditions were identified as social networking groups that are increasingly being developed and used which could cause an increase in threats to CBIS and potential loss of data from attacks. Computer disasters could, therefore, adversely affect information management that in turn affects the effectiveness, profitability and competitiveness of an organization.

As the need for information grows, so does the criminals' methodology in manipulating the data and information held in computers. According to Forcht and Pierson (1994), computer crimes such as manipulation of data, alteration of data order, counterfeiting, false propaganda, falsification of data, holding computers hostage, victimization of point of sale terminals and hacking are growing worldwide and threatening information systems.

Library computers and networks are subject to both natural and man-made disasters. It is, therefore, essential to plan for disaster in order to protect computers and networks where possible and to recover from disaster as quickly as possible if and when disaster does occur. Disaster planning for computers and networks is, therefore, important because these technologies are essential in offering efficient and effective patron service and enhancing staff productivity. According to Boss (2006), the only access many people have to the internet is through their library. Libraries have become dependent on these technologies for ordering, claiming and receiving, charging and discharging of library materials to patrons, and their provision of reference services. Hence, every hour of downtime is extremely serious, and a library must give disaster planning a high priority.

Boss (2006) defines disaster as "a sudden misfortune that is ruinous to an undertaking." There is little time to react at the time of the misfortune. Hence, preparations have to be made in advance and the focus should be on disaster

planning which entails various activities such as risk assessment (what is the probability that a particular disaster will occur and how serious is the effect likely to be if it does occur?) and risk-reduction (lowering the risk factor by reducing the probability, reducing the effect, or both).

2.4.2 Security Measures for Computer-Based Information Systems

According to Fitzgerald and Dennis (2002), securing a computer-based information system means developing controls which are the mechanisms that reduce or eliminate the threats to network security. There are three main types of controls that prevent, detect and correct whatever might happen to the organization through the threat faced by its computer-based systems. As Fitzgerald and Dennis (2002) note, preventive controls are defined as those that mitigate or stop a person from acting or an event from occurring such as use of password, guard and security lock. Detective control reveals or discovers unwanted events such as use of software. Corrective controls remedy an unwanted event or a trespass. Either computer programmes or humans verify and check data to correct errors or fix a security breach so that it does not recur in future.

The key principal in preventing disruption, destruction, and disaster, or at least reducing impact, is redundancy (Fitzgerald & Dennis (2002). Redundancy can be achieved through various methods as pointed out by Chow and Ha, 2009; Fitzgerald and Dennis, 2002; Rhode and Haskett, 1990; which include the following:

i. **Battery backup:** - According to Chow and Ha (2009), battery backup is important since computer hardware is energy or power dependent and this was also echoed by (Fitzgerald & Dennis, 2002).

ii. **Data, documents, data files and mails backup** provide redundancy to facilitate recovery after a disruption, corruption or disaster has occurred (Chow & Ha, 2009). Backup storage according to Rhode and Haskett (1990) refers to how all relevant IS data has been copied and kept in a safe place from which it can, when needed, be retrieved quickly for restoration echoes (Chow & Ha, 2009). Data backups are a major component of disaster control planning and a detailed plan of backing up is vital and must cover issues of frequency, type and location. It must also be kept secure from damage. Eden and Matthews (1997) recommend backup of computer systems, software and files.

iii. **Hot site and cold site –** A site in this case is an alternative location where operations of an organization are carried out when a disaster strikes. A hot site, therefore, provides for instantaneous (or nearly so) recovery of the original site. This is done by completely replicating the original site in terms of the computing infrastructure and operations of the organization off-site. Thus, when the main system fails, the hot site immediately takes- over the operations of the organization. A cold site provides the same basic type of infrastructure as hot site, but does not replicate in real-time the operations of the main site. A certain amount of setup must occur in order to switch operations over after a disaster occurs (Cervone, 2006). Chow and Ha (2009) observe that firms that highly depend on IS applications must consider an alternative site with which they can backup their resources and databases so that they can be recovered easily in the event of a disaster which is also echoed by (Hawkins et al., 2000). This can be implemented in a mode of hot site, a cold site, mobile recovery facilities, a mirror site (Hawkins et al.,

2000) which can be done either externally or in-house (Fitzgerald & Dennis, 2002).

iv. **Servers:** **Fault tolerant** servers that contain many redundant components to prevent failure can be used such as disk mirroring which uses a second redundant disk for every disk on the server. Every data item written to the primary disk is automatically duplicated on the mirrored disk. Fitzgerald and Dennis (2002) observe that if the primary disk fails, the mirrored disk automatically takes over.

Measures taken to secure computers and CBIS have been addressed in literature. A gap still exists on measures taken by libraries to secure their CBIS. This is especially so in Kenya. The Study hoped to fill this gap by establishing measures taken to prepare and mitigate for disasters which affect CBIS in libraries.

2.5. Personnel In-charge of Disaster Management

Disaster recovery planning is considered to be one of the most critical management issues for both private and public organizations in our present age of digitization observe (Chow & Ha, 2009). Unfortunately, disaster management seems to be one of those managerial activities which are put off until a later date, often because the likelihood of experiencing a disaster is thought to be so remote, observe (Eden & Matthews, 1997). Chow and Ha (2009) quoting Elstain (1999), continue to say that a halt of any information system function service may truly be devastating for the operational capacity and reputation of an organization. Loch et al (1992) note that management recognizes that threats to continuing operations to include technological issues seldom previously considered. Thus, protecting a corporation's information system and data warrants management attention. Therefore, putting an effective DRP in place can reduce the severity of a potential disaster and can

speed up the recovery processes where necessary (Chow & Ha, 2009 quoting Rutherford & Myer, 2000).

Fitzgerald and Dennis (2002) point out that it is not enough to just establish a series of controls, someone or some department must be accountable for the control and security of the network. This includes being responsible for the developing controls, ensuring they are operating effectively, and determining when they need to be updated or replaced. Chow and Ha (2009), therefore, identified top management commitment as one of the major factors for DRP for information system functions in an organization. Ginn (1989) as quoted by Chow & Ha (2009), states three reasons why top management commitment is considered the most vital construct to the success of DRP in an organization as: finalizing an annual budget to support DRP implementation, deciding when and how the DRP should be implemented, and dictating the level of co-operation and support that should be provided by the various departments when a DRP is launched.

According to Chow (2000), top management is considered as critically important as DRP involves ongoing capital investment and requires long-term planning. Chow and Ha (2009) also pointed out other reasons why top management is seen as important for the success of DRP which include: providing adequate financial support for DRP development, commitment to DRP development, supporting DRP development, accepting responsibility for DRP quality of and being in charge of forming and appointing the steering committee so that all functional units offer their full co-operation.

As noted by Loch et al., (1992), the growth of connectivity and diversion of technology with or between organizations will continue. IS security therefore, remains high on the list of key issues facing information systems executives.

Hence, management needs to become more informed of the potential security breaches in the system via employees and competitors. Increase its awareness in key areas and recognize that its overall level of concern for security could underestimate the potential risk inherent in the highly connected environment in which it operates.

According to Wong et al., (1994) as quoted by Chow & Ha (2009), top management is responsible for setting up a DRP committee that should consist of representatives from each functional unit so that their views on critical DRP events can be accurately gathered. Chow & Ha (2009) and Wong et.al (1994), claim that information system function personnel must participate and monitor the development processes of DRP in an organization. They should contribute their technical knowledge at all different stages. They should review the plans regularly from a technical standpoint so that minimum service disruption is sustained (Rutherford & Myer, 2000).

It is important for the IT manager and ISL to work together in order to ensure computer-based information systems in the library and the organization are well-protected against disaster and are well-prepared for disaster if it occurs. Eden and Matthews (1997) point out the importance of liaison between library IT personnel, internal computing department and service providers in establishing security and recovery requirements, temporary service and access arrangements for CBIS as a way of preparing for disaster.

IT managers and system librarians should be in a position to carry out risk assessment, which entails knowledge relating to their buildings, computing systems and equipment or electrical systems, the consequent risks to people, collections among others, in order to be able to prevent disasters (Eden &

Matthews, 1997). This will enable the personnel to adequately handle disaster-related issues for computer-based information systems.

The involvement of several personnel in ensuring that DRP in an organization takes place has been documented in literature. A gap exists on the education and skills of persons involved in ensuring security of CBIS which the study hopes to fill and especially in libraries.

2.6 Disaster Management Plans, Policies and Programmes

Loch et al., (1992) note that the ultimate aim of any computer security policy must be to protect the integrity, availability, and confidentiality of the electronic data held within the system. They continue to note that we protect systems and data from the risk of change or destruction or risk due to the presence of threats. A DRP policy must be clearly outlined and be made clear to everyone in an organization (Chow & Ha, 2009). They continue to note that it is important to establish policy and goals for an effective DRP in an organization. The purpose of a policy statement is to set the guidelines for disaster recovery and define who is accountable for the DRP planning process (McNurlin, 1998 as cited by Chow & Ha, 2009; Turner, 1994). The DRP policy statement should clearly define realistic goals and their objectives (Chow & Ha, 2009). With clear goals and objectives, recovery strategies can be established in a cost-effective manner (Rothstein, 1998 as cited by Chow & Ha, 2009). There is need for effective data backup policies as well as policies and programmes addressing training for organization employees on disaster prevention and recovery.

2.6.1 Disaster Management Plans

Klein and Joseph (2007) argue that all businesses need a DCP to deal with uncertainties or disasters. Disaster Control Planning involves the formulation

of a written plan which gives details of preventive and preparatory measures intended to reduce potential risks, and which also indicates reactive and recovery procedures to be taken in the event of a disaster (Eden & Matthews, 1997).

It would be foolish and naive to think that we can totally prevent disasters, as we cannot. We can, however, do a great deal to prevent some of disasters from happening, reduce their effect on the collections when they do happen and to minimize the damage caused. To do this, it is necessary to apply preventive measures, to establish emergency procedures, hold emergency equipment and supplies in readiness, arrange for the necessary backup services to be available and for staff and disaster teams to be fully conversant with, and trained in disaster reaction. In short, disaster management plans (Kibaru, 2005).

The value of a disaster control plan is the ability to react and recover from an incident swiftly and efficiently. Since disasters occur for a number of reasons both routine and dramatic plans must be put in place to address every aspect of operations. During the development of the plan, three major aspects have been identified as: initial planning, development of the infrastructure and testing of the plan.

One of the best ways to get started in planning is to conduct a Business Impact and Risk Analysis (BIRA). This involves asking a series of questions such as: Which processes are the most critical? What vulnerabilities does the library face? How can the library mitigate risks related to the vulnerabilities?

BIRA helps the planning team to identify the critical business functions within the organization and what the impact would be if each of the identified functions were not performed. BIRA helps people focus on what can be done

to reduce risk before an event, how people should respond when an event occurs, and how to recover after an event.

BIRA can also be used as a development and awareness exercise as it helps dispel some of the myths that may exist within the organization related to disaster recovery and preparedness (Carvone, 2006). He further notes that plans must be reviewed periodically to ensure they are still useful. They should also be verified and tested. Verifying ensures that the plans are present, and testing determines whether the plans are working as originally specified.

2.6.2 Importance of DCP

It is important when developing a plan to remember the objectives of DCP as outlined by Eden and Matthews (1997) as follows:

i. To prevent the event from occurring.
ii. To protect material in case the event occurs.
iii. To salvage damaged material with sufficient speed and efficiency so that its condition can be stabilized.

2.6.3 Elements of a Disaster Control Plan

According to Eden and Matthews (1997), disaster management needs to be carefully considered and properly planned, and all staff should be made aware of the risks to the items in their care and what is expected of them if a disaster occurs. The four stages in the disaster control planning process identified by Eden and Matthews (1997) are: prevention/mitigation, preparedness, reaction, and recovery.

2.6.3.1 Prevention

Taking preventive measures to reduce risk is vital. The first step in disaster prevention is risk assessment. Other issues include: regular inspections of buildings and equipment, fire detection and suppression systems, proper

storage of equipment (Eden & Matthews, 1997). For CBIS, this may include regular blowing of computers, avoiding liquid spills, air conditioning especially in server rooms, access controls, regular updating of software such as anti-viruses.

2.6.3.2 Preparedness

Corvone (2006) identified some key important areas related to disaster preparedness such as developing emergency operation plans, training key staff members that are responsible for emergency response functions as well as institutionalizing incident response command systems. Eden and Matthews (1997) observe that no matter how carefully risks are assessed and preventive measures taken, and no matter how diligent staff are in carrying out their responsibilities, disaster may still occur. They advise that disaster control plans should be drawn, be revised regularly, people responsible for drawing up the plan liaise and negotiate with staff from other departments in the organization, carry out staff training, make a list of suppliers of emergency services and equipment, make an inventory of collections and equipment, make backup of documents, check for insurance cover and what is offered, and arrange for temporary services, accommodation and storage.

2.6.3.3 Reaction

Reaction refers to turning the preparations which had already been made into some kind of response (Eden and Matthews, 1997). They continue to observe that having the right people to put the disaster control plan into action is absolutely essential as these are the people who may have to take responsibility for their own actions and the actions of others in the extremely stressful circumstances. Further, expert advice and a record of what was done are also needed during the reaction period after disaster strikes.

2.6.3.4 Recovery

Carvone (2006) notes that disaster recovery planning is a critical component of a digital library system infrastructure that is often overlooked. He continues to note that it is unfortunate because the consequences of being unprepared for disaster are significant. Disaster Recovery planning as it relates to library falls into three major areas (Carvone; 2003). These are:

- Safety and wellbeing of employees and patrons.
- Coordination of recovery activities.
- Recovering critical business functions.

The principles that guide the plan include;

- Limiting disaster related damages.
- Mitigating financial losses and legal liabilities.
- Minimizing the costs of recovery operations.

2.7 Challenges in Securing CBIS

Nyandiere (2007) points out various challenges faced by higher education institutions in a bid to implement information systems which include lack of awareness and mindset among staff, lack of top level management commitment, lack of appreciation of ICT, poor strategy in making ICT responsive to organizational vision and mission, lack of a systematic method of system implementation. This in effect affects preparedness for disaster related to CBIS. Other challenges that Nyandiere (2007) cites are inhibiting cost of hardware and software, and funding for sustainability and continuity in maintenance and replacement of equipment as well as increasing technology. Chacha (2005), as cited by Nyandiere (2007), notes that insufficient training and re-skilling of end users as well as technical staff who support the systems

is a major challenge to CBIS. In addition, there is also the problem of recruitment and retention of qualified information systems staff.

Technology complexity brings the challenge of security concerns for data and systems especially where users have to access institutional systems. Without proper controls, users can hack into an organization's systems and change or modify them.. In the current networked-centric business model, it is becoming increasingly difficult to validate a person's identity, control access, and maintain integrity and privacy of data (Tran, 2006). Tran (2006) notes that security is a multi-faceted problem that requires close analysis of all the vulnerable factors in a business infrastructure. Laundon and Laundon (2000) identified large number of online users and ease of exploiting flaws in web applications as other challenges.

2.8 Summary

From the literature it was found out that libraries experience both natural and man-made disasters (Kaur, 2009; Shaluf, 2007; Cervone, 2006; Eden & Matthews, 1997). A number of authors have carried out research and identified various disasters that may affect libraries and the need to have disaster management plans and programmes to ensure the library continues to run even after a disaster happens. These studies concentrated on security issues of the library buildings, printed collections, and disasters such as flooding, fire and theft (Wambiri, 2008; Aziagba and Eden, 2008; Kimani, 1998). Not much has been done to study preparedness and mitigation for disaster that might affect library CBIS which is a critical aspect in this era of information technology. The researcher, therefore, sought to fill this gap by addressing disaster management issues for computer-based information

systems in the libraries given that university libraries have continued to automate their services and operations.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

Kothari (1985) defines research methodology as a way of systematically solving the research problem. It involves the logic behind the methods used in the context of the research study and an explanation of the preference for a particular method or technique so that research results are capable of being evaluated by the researcher. This Chapter covers the methods and procedures used to conduct the research. It basically covers the research design, variables, study population, sampling procedures, data collection techniques, tools of data collection, piloting and quality assurance as well as data analysis and interpretation methods.

3.2 Research Design

According to Creswell (2009), research designs are plans and procedures for research that span the decisions from broad assumptions for detailed methods of data collection and analysis. The decisions involve the design to be used to study a topic, which entails worldwide assumptions the researcher will bring to the study, procedures of enquiry, specific methods of data collection, analysis and interpretation (Creswell, 2009; Gay et al., 2009).

Exploratory and descriptive survey research designs were used in this study. Exploratory research design was used because there was need to understand the issue of disaster management relating to CBIS in university libraries in Kenya since little if anything has been documented on this issue. This type of approach was preferred because the topic was relatively new. It had not been explored or addressed with the sample or group of people involved in this

research Mure (1991) gives several characteristics of an exploratory research design noting:

> the concept is "immature" due to a conspicuous lack of theory and previous research; a notion that the available theory may be inaccurate, inappropriate, incorrect, or biased; a need exists to explore and describe phenomena and to develop theory and the nature of the phenomenon may not be suited to quantitative measures.

Most of the data collected did not allow quantitative analysis and exploratory design was therefore appropriate for this study. In qualitative research design approach, Creswell (2009) and Gay et al., (2009) note that a researcher gathers multiple forms of data through interviews, observations, documents, rather than rely on single data source. The researcher used several data collection methods which included observations, interviewing, document analysis, audio-recording and photographing. The descriptive survey research design was used in the study because some of the data collected generated data that could be analyzed using descriptive statistics.

3. 3 Variables

According to McBurney (2010), a variable is some aspect of testing condition that can change or take on different characteristics with different conditions. A dependent variable is a measure of the behaviour of the subject and the independent variable is one that is believed to cause some change in the value of the dependent variable.

3. 3.1 Dependent Variables

The dependent variables in the study was disaster preparedness which depends on mitigation factors such as measures taken to secure CBIS, Training of personnel involved and skill and education of the personnel involved in securing CBIS.

3.3.2 Independent Variable

The independent variables in the study were mitigating factors. These variable influence disaster preparedness and hence, response and recovery in case of a disaster.

3.3.3 Intervening Variables

The intervening variables in this study included the hazard assessment and risk mitigation. These guide in the mitigation factors that should be put in place to facilitate disaster preparedness.

3.4 Location of the Study

The study was carried out in Nairobi County and the neighbouring counties. Public and fully-chartered private universities made a good representation of the universities in Kenya and provided the required information. Two public and two fully-chartered universities were selected for the study. The selected universities had introduced Open University: distance, e-learning and part-time programmes which require an efficient and effective library ICT infrastructure since the target group in these programmes comprises learners who are separated from the main institution by either time or location and need access to library resources and services wherever they may be. Such learners require systems that are running almost all the time. Further, the selected universities were ISO certified and therefore, had passed some measures of quality in terms of provision of services. In order to explore and have an insight and better understanding of the issues relating to disaster management for CBIS in the libraries, the researcher believed the four selected universities could form a basis for providing the required information. The results of the study were not to be generalized to other cases since each institution was unique and therefore exploratory research design was suitable

for this study and the four sites were considered adequate to provide relevant information to meet the study objectives and research questions.

3.5 Target Population

Gay (2009) defines study population as the larger group from which a given sample is selected. The study sites were two public universities and two fully-chartered private universities within Nairobi County and its neighbouring counties.

The study population comprised only those members of staff that were employed on permanent basis and not the casual employees. Further, the support staffs in the library were not considered for the study. The public universities and fully-chartered private universities in Kenya were as shown in Table 3.1:

Table 3.1: Public universities and fully chartered private universities in Kenya

PUBLIC UNIVERSITIES	FULLY CHARTERED PRIVATE UNIVERSITIES
1. Kenyatta University	1. University of Eastern Africa, Baraton
2. Moi University	2. Catholic University of Eastern Africa
3. Egerton University	3. Daystar University
4. Jomo Kenyatta University of Agriculture and Technology	4. Scott Theological College.
5. University of Nairobi	5. United States International University
6. Masinde Muliro University of Science & Technology	6. Africa Nazarene University
7. Maseno University	7. Kenya Methodist University
	8. St. Paul's University
	9. The Pan Africa Christian University
	10. Kabarak University
	11. Strathmore University

Source: Commission for Higher Education Website 2012

From the four selected universities the target population was as shown in Table 3.2.

Table 3.2: Target population

UNIVERSITY	ICTD	NUMBER OF STAFF IN THE LIBRARY	TOTAL
R	**1**	42	43
S	**1**	32	32
T	**1**	22	23
U	**1**	17	18

Source: University librarians of the respective universities (2012)

The data elements from the selected universities were the university librarians, deputy university librarians, the information systems librarians, IT managers, library ICT technicians, and circulation librarians.

3.6 Sampling Techniques and Sample Size

Sampling is the process of selecting a small number of individuals for a study in such a way that the individuals chosen will be good key informants who will contribute to the researcher's understanding of a given phenomenon (Gay et al., 2009). Samples in exploratory research were generally smaller and less representative allowing in-depth interview method. The researcher's intent was to describe a particular situation in-depth and not to generalize. Representativeness was, therefore, secondary and the goal was to select participants who could best add to the understanding of the phenomenon under study (Gay et al., 2009; Creswell, 2009). Since the research design chosen was mainly exploratory, key informants were purposely selected from the selected universities.

3.6.1 Purposeful Sampling Technique

In qualitative research, such as exploratory research design, participants, documents, visual aids or materials, and location of study were purposefully selected that would best assist the researcher understand the problem under study. Hence, the researcher relied on experience and insight to select a sample for the study (Gay et al., 2009; Creswell, 2009).

Exploratory research design technique was used since it enabled the researcher select participants who would best answer the research questions and meet the research objectives. At the same time, groups of employees in the selected universities who had information related to the study were known. Therefore, purposive sampling technique was used to select the location and the participants for the study.

3.6.2 Sample Size

In qualitative research, there are no hard and fast rules to specify number of participants. Qualitative studies can be carried out with a single participant or with as many as 60 or 70 participants representing multiple contexts. A sample of more than 20 is large enough (Gay et al., 2009; Creswell, 2009). Saunders (2003) notes that research questions and objectives that do not require statistical estimation should have a sample smaller than 30 participants. Gay (2009) also notes that having more participants does not necessarily mean the study or its results will be more reliable or more useful. A total of 26 respondents were selected to participate in the study as shown in the Table 3.3 below.

Table 3.3: Sample size

UNIVERSITY	ICTD	NUMBER OF STAFF IN THE LIBRARY	SAMPLE SIZE
R	1	42	7
S	1	32	7
T	1	22	7
U	1	17	5
Total	**4**	**113**	**26**

Source: University librarians of the respective universities (2012)

From Table 3.3 above, the sample distribution was as in Table 3.4:

Table 3.4: Representation of respondents

UNIVERSITY	UL	DUL	ICTD	ISL	ICTT	CL&OL	TOTAL
R	1	1	1	1	1	2	**7**
S	1	1	1	1	1	2	**7**
T	1	1	1	1	1	2	**7**
U	1	-	1	-	1	2	**5**
Grand Total	**4**	**3**	**4**	**3**	**4**	**8**	**26**

Source: University librarians of the respective universities (2012)

KEY: UL-University Librarian, DUL-Deputy University Librarian, ISL-Information Systems Librarian, ICTD-Information Communication and Technology Director, CL-Circulation Librarian, ICTT-Information Communication and Technology Technician in the library, OL- One Other Library staff.

3.7 Research Instruments and Equipments

To meet the research objectives, the researcher developed the following instruments; interview schedules, observation checklist and a list of documents to be collected.

3.7.1 Interview Schedules

According to Bordens (1996), an interview is a method of administering a questionnaire that involves face- to- face interaction with the subject. According to Gay (2009), the interview method of data collection has the following advantages: useful when participants cannot be directly observed, participants can provide historical information and allows researchers control over the line of questioning.

Unstructured and semi-structured questions were prepared and used to elicit views and opinions from the participants. These were mainly targeted at the UL, DUL, ISL, ITCD, ICTT and CL. The interview schedule was prepared in line with the study objectives and the research questions. The information sought helped meet the study objectives. As a validity check, the researcher used telephone interviews for clarification on issues that were not clear during transcription or as a way to confirm given information.

3.7.2 Observation Checklist

According to Kombo (2006), observation is a tool that provides information about actual behaviour. Direct observation allows the researcher to put behaviour in context and thereby understand it better. According to Gay (2009), advantages of observation include: researcher has first-hand information, he/she can record information as observed, unusual aspects can be noticed during observation, and useful for exploring topics that may be uncomfortable for participants to discuss.

The researcher prepared an observation checklist of items to be observed and used it in computer rooms and server rooms as well as any other place where computers were located in the library. The researcher carried out the observations after the interview sessions. This worked as a validity check to confirm some of the information given during the interviews. The observation checklist was used to observe security measures in place for equipment such as computers which included use of guards, clocking, lock and key, air conditions of server rooms, among others. See appendix A (page 159) for items observed.

3.7.3 Secondary Information Sources Check List

Secondary information sources are data neither collected directly by the user nor specifically for the user. They involve gathering data that already has been collected by someone else. This is the collection and analysis of published material, and information from internal sources (Kombo, 2006).

According to Gay (2009), using secondary sources of information is advantageous because researchers obtain the language and words of participants, can be accessed at a time convenient to the researcher – unobstructive source of information, represents data which is meaningful in

that participants have given attention to compiling it, as written evidence. It saves the researcher time and expense of transcribing.

Secondary information sources that were used included policies and strategic plans of the organizations and those of the institutional libraries. These gave details on disaster prevention, preparedness, reaction and recovery procedures for CBIS as well as content coverage, persons responsible, and their responsibilities.

3.7.4 Audio-Visual Data Capture Equipment

Audio-visual materials may include photographs, videotapes, art objects, computer software, film, and audio tapes. These materials are advantageous in that they may be unobtrusive methods of collecting data. They provide an opportunity for participants to directly share their reality and they are creative in that they capture attention visually. These materials were produced by the researcher during data collection through audio, video-taping and photography. This strategy was used during interviews and observations. The researcher used a video camera to capture relevant scenes as was observed from the site. An audio recorder was used to capture the interview conversations. This was done only after consent was granted by the interviewee.

3.8 Pilot Study

Piloting is a small scale trial of the study conducted before the full-scale study. It is used to identify unanticipated problems or issues. Pilot testing of the instruments provides information about deficiencies and suggestions are given for improvements (Gay, et al., 2009; Glense, 2006).

Piloting was done in one of the universities in Nairobi County and which had not been selected for the study. Five senior members of staff in the library

conversant with ICT were selected and interviewed to check the correctness and completeness of the instruments. Observations were also carried out in the essential area where computers were located such as the server room and offices. This enabled the researcher to refine the observation checklist and the interview schedule.

3. 9 Quality Assurance

Validity is concerned with whether the data or information gathered is relevant to the decision being made, which means the degree to which a test measures what it is supposed to measure (Gay et al., 2009; Creswell, 2009). In exploratory research, the common terms used to describe validity and reliability are trustworthiness, dependability and understanding.

According to Maxwell (1992), as quoted by Gay et al., (2009), trustworthiness and understanding can be achieved by addressing descriptive validity (factual accuracy of the account), interpretive validity (meaning attributed to the behaviours or words of the participants), theoretical validity (how well the research report relates to the phenomenon under study to a broader theory) and generalizability and evaluative validity (whether the researcher was objective enough to report the data in an unbiased way, without making judgments and evaluations of the data).

To ensure validity, the researcher reported the data objectively Triangulation was used to obtain a more complete picture of the disaster management for CBIS in libraries. This included interviews, observations and document analysis. Triangulation was used to cross-check the information given from different data collection methods that were used. Follow-up interviews were done through telephone to confirm responses and check consistency of information given.

To ensure dependability or trustworthiness, the researcher collected detailed descriptive data and ensured that there was no distorting anything seen or heard, or makeup events based on inferences. The researcher ensured that data analysis and interpretations accurately reflected the documents' recordings, films, and other primary sources of data collected as part of the study. During interviewing, probing was used to get in-depth information. Observations were recorded as accurately as possible and this was done as soon as possible to avoid forgetting. Photography and audio taping were used to ensure collected data was not distorted. Audio and visual recordings were used to facilitate accuracy during the analysis.

3. 10 Data Collection Technique

The researcher sought permit to carry out research, see Appendix F on page. Once this was granted, the researcher collected data as follows:

For interviews, the researcher booked appointments with the selected participants. During the interviews, the researcher took notes and audio-recorded the interviews. Observations were carried out after the interview session. This was used to clarify some of the issues raised during the interview. Documents identified during the interviews (see Table 4.6 on page) were either collected after the interview sessions, downloaded from the university websites or were emailed by the respondents.

3.11 Data Analysis

According to Oso and Onen (2005), data analysis deals with its organization, interpretation and presentation. It is the complex process of selection, sharpening, sorting, focusing, discarding and organizing in order to make

sense out of the data, integrating it, drawing conclusions and verifying it (Miles & Huberman, 1994).

Collected data was organized and prepared for data analysis. This involved transcribing interviews, optically scanning the materials, typing field notes, sorting and arranging the data into different types depending on the sources of information. The researcher read through the data to initially obtain a general sense of the information and to reflect on its overall meaning.

Detailed analysis was then done using a coding process which entailed organizing the material into chucks or segments of text before bringing meaning to information. It involves taking textual data or pictures gathered during data collection, segmenting sentences or paragraphs or images into categories, and labeling those categories with a term, often a term based on the actual language of the participant (Creswell, 2009). In this case numeric codes were used to categorize data according to the identified themes.

The researcher analyzed the collected data by organizing it into themes that were derived from the research objectives and the research questions. Documents were read and analysed according to issues raised pertaining to the research objectives and research questions. Narratives were used to report findings and some data was presented in Tables of frequency distributions, percentages, pie charts and plates.

3.12 Ethical Considerations

According to Israel and Hay (2006), as cited by Creswell (2009), researchers need to protect their research participants, develop a rapport with them, promote the integrity of research, guard against misconduct and impropriety that might reflect badly on their organizations or institutions. Ethical issues

also deal with personal disclosure, authenticity and credibility of the research report (Creswell, 2009).

Ethics in this study was ensured through the following:

- Informed consent. Participants were informed of the purpose of the research and were only interviewed once they agreed to participate.

- Guarantee of confidentiality to the participants. Real names were not used in the report. In coding and recording process, the researcher disassociated names from responses. The researcher, therefore, used aliases, pseudonyms for individuals and sites to protect their identities. Thus for sites, letters of the alphabet R, S, T and U were used to represent them during reporting. For individuals aliases, were used as shown by use of an asterik (*) against the name.

- Where the participants requested the results of the findings, the researcher shared them.

- The researcher did not suppress, falsify or invent findings to meet any specific or particularized needs.

- Permission to carry out the research in any given institution was sought from relevant authorities.

- Researcher made appointments with the interviewees and interviewed them at their convenient place and time. The researcher explained to the interviewee the purpose of research and guaranteed confidentiality of information given.

- Interviews were only audio-recorded with permission from the interviewees. For those who declined, the interview was not audio-recorded.
- The researcher only took photographs after permission was granted by interviewees.

CHAPTER FOUR

FINDINGS, INTERPRETATION AND DISCUSSION

4.1 Introduction

This Chapter analyses data gathered through interviews, observations and document analysis. The raw data collected was organized in a meaningful and useful form to allow for conclusions to be drawn. The Chapter focuses on the various themes which were derived from the research objectives, research questions, and the assumptions of the study. The themes were categorized as follows:

Key themes

i. Automation in libraries, electronic information resources and services.
ii. Awareness and perception of CBIS.
iii. Awareness, understanding and perception of security for CBIS.
iv. Threats experienced in libraries related to CBIS.
v. Measures used to prepare and mitigate disaster for CBIS.
vi. Indicators of unpreparedness for disaster related to CBIS.
vii. Personnel involved in disaster preparedness and mitigation for CBIS.
viii. Policies, programmes and plans on disaster preparedness and mitigation for CBIS.
ix. Challenges associated with disaster management for CBIS.

4.2. Distribution of the Respondents

The participants were drawn from two public universities and two fully-chartered private universities within Nairobi County and its neighbouring counties. The distribution was as shown in the Table 4.1 below:

Table 4.1: Distribution of the universities

UNIVERSITY	TYPE
R	Public

S	Public
T	Private
U	Private

SOURCE: Commission for Higher Education Website (2012)

From Table 4.1, the targeted participants were as shown in Table 4.2 below. These were the participants the researcher believed to have the relevant information on the topic of the study.

Table 4.2: Targeted respondents

UNIVERSITY	UL/or DUL	ISL	ICTT	CL &OL	ICTD	TOTAL
R	2	1	1	2	1	**7**
S	2	1	1	2	1	**7**
T	2	1	1	2	1	**7**
U	1	-	1	2	1	**5**
Grand Total	**7**	**3**	**4**	**8**	**4**	**26**

Source: University librarians of the respective universities (2012)

KEY: UL-University Librarian, DUL-Deputy University Librarian, ISL-Information System Librarian, ICTT-Information Technology Technician, CL-Circulation Librarian, OL-One other Librarian, ICTD- Information Technology Director

During data collection, the researcher observed that all the circulation librarians from the selected universities had been in their respective libraries for a period ranging between 8 to 20 years. In this case, the researcher interviewed the CL only and, therefore, OL was excluded from the interview. The researcher believed that 8 to 20 years was sufficient for the circulation librarian to have experience or witnessed any disaster that could have occurred in the library and affected the CBIS. This was not in any way going to compromise the reliability and validity of the study since the circulation librarian gave the required information. The researcher carried out interviews as shown in Table 4.3. From Table 4.3, the ICTD/T was introduced into the list of respondents because this respondent was believed to have the necessary information and therefore, accompanied the ICTD during the interview. The researcher considered that either the UL or the DUL would be sufficient to provide the information sought and, therefore, there was no need to interview

both of these two officials. Table 4.3 shows the distribution of respondents that were interviewed:

Table 4.3: Interviewed respondents

UNIVERSITY	UL	DUL	ISL	ICTT	ICTDT	CL	ICTD	TOTAL
R	-	-	1	1	-	1	1	**4**
S	1	-	1	1	-	1	1	**5**
T	-	1	1	1	1	1	1	**6**
U	1	-	-	1	-	1	1	**4**
Grand Total	**2**	**1**	**3**	**4**	**1**	**4**	**4**	**19**

SOURCE: Interviews

4.2.1 Characteristics of the Respondents

This section comprises the analysis of the respondents by gender, age, qualification and position held. The respondents were drawn from employees holding managerial positions and/or ICT related positions. Therefore, it is important to have clear understanding of the characteristics of respondents dealt with.

a) **Distribution of respondents by gender**

The study revealed that majority of the respondents were male at 84% while female were at 16% as shown in Figure 4.1 below. Since the respondents were drawn from managerial and ICT related positions, this implied that these two positions were male dominated.

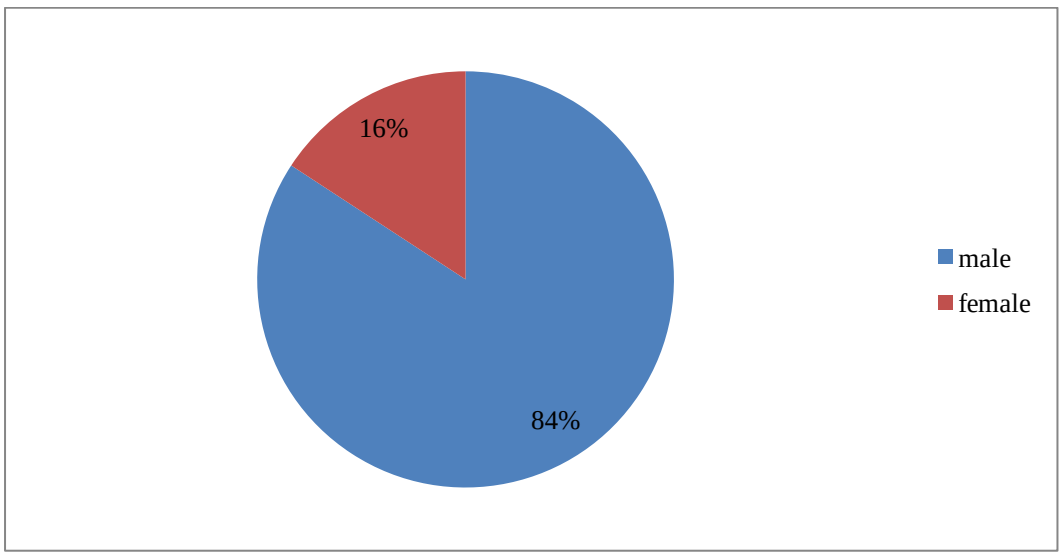

Figure 4.1: Distribution of respondents by gender. ***Source: Interview data***

b) Distribution of Respondents by Age

The study revealed that majority of the respondents were between 41-50 years at 32% followed by those above 50 years at 26 %. This meant that most of the respondents were 40 years and above at 58% while those below 40 years were at 42%, where those between 30-40 years were at 21% and those below 30 years were at 21%. This was as shown in Figure 4.2 and 4.3 below:

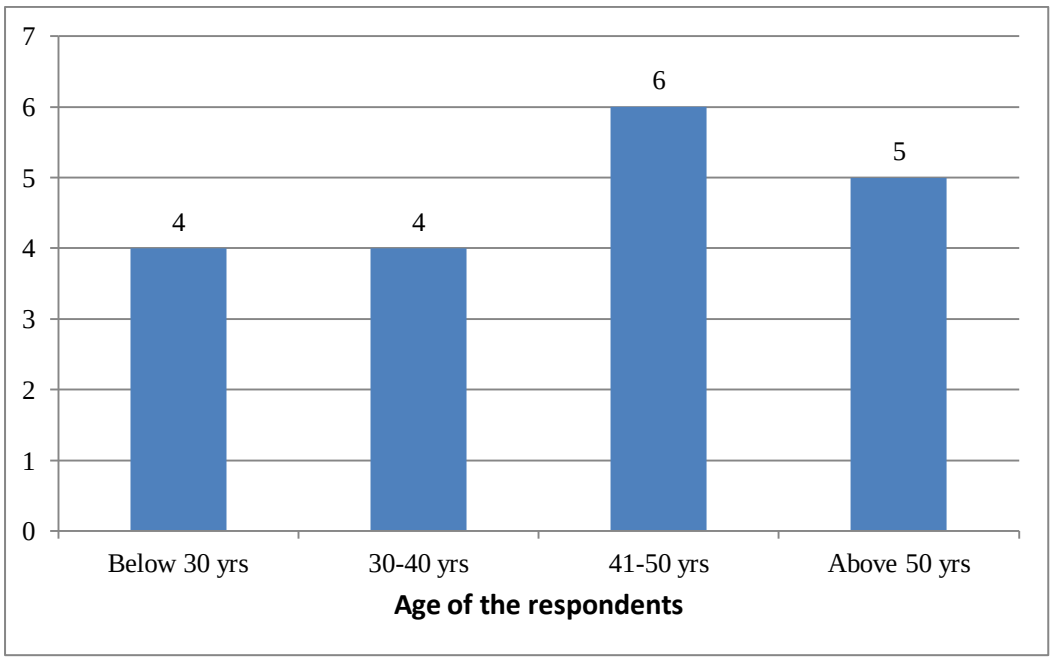

Figure 4.2: Distribution of respondents by age. ***Source: Interview data***

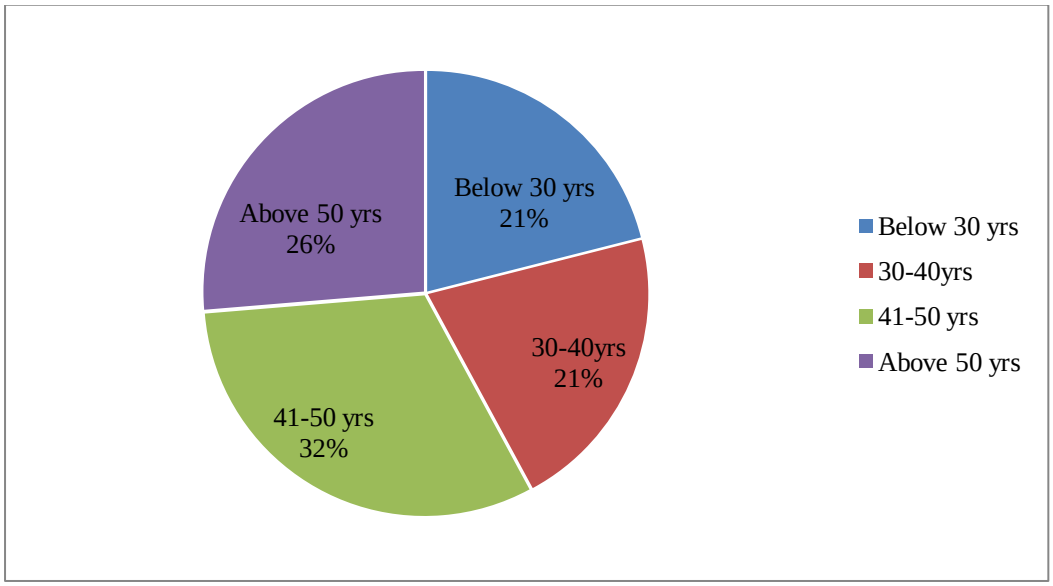

Figure 4.3: Percentage distribution of respondents by age. ***Source: Interview data***

c) Distribution of Respondents by Qualification

The respondents comprised highly qualified personnel given that 95% of the respondents had a Bachelor's degree and above. In fact, 47% of the respondents had a Master's degree and only 5% had a diploma. This is as shown in Figure 4.4:

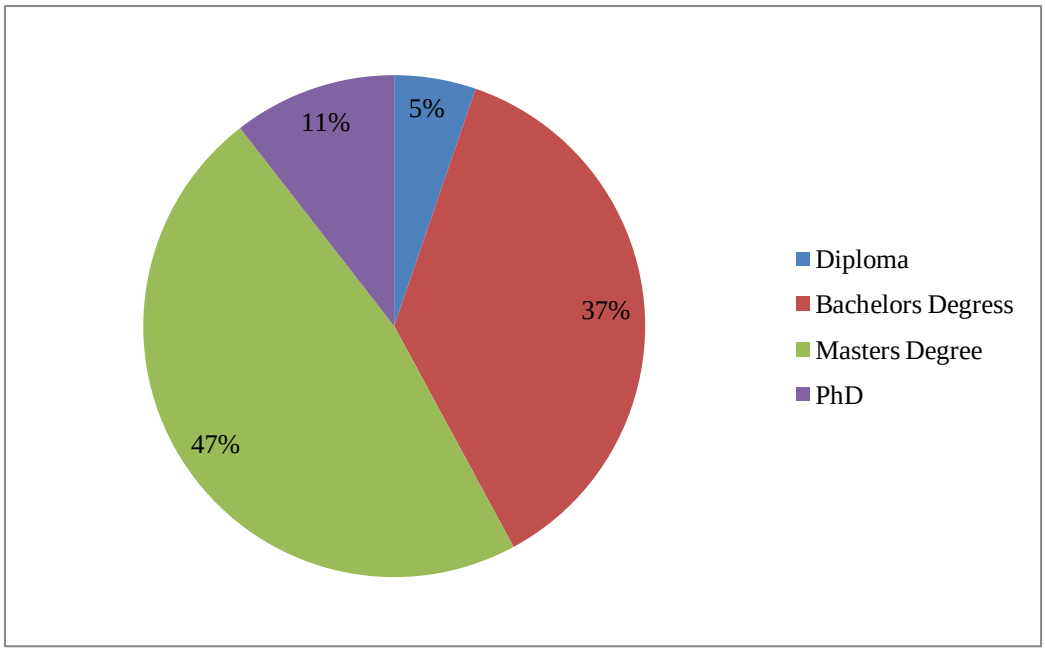

Figure 4.4: Distribution of respondents by qualification. ***Source: Interview data***

d) Distribution of Respondents by Position and Qualification

The researcher sought to find out the distribution of respondents by position and qualification. This was meant to shed light on the calibre of people who maintained the CBIS in the library in a view of establishing whether they were qualified academically, and, what position they held which could influence the decisions made about CBIS. The distribution was as shown in Table 4.4:

Table 4.4: Distribution of respondents by position and qualification

Position/ Qualification	Diploma	Bachelor's Degree	Master's Degree	P.hD
CL	-	2	2	-
UL&DUL	-	-	2	1
ICTD	-	-	4	-
ISL	1	-	1	1
ICTT&ICTTD	-	5	-	-
TOTAL	**1**	**7**	**9**	**2**

Source: Interview data

e) **Distribution of Respondents by Position and Age**

The researcher sought to find out the respondents' distribution by their position and age as shown in Table 4.5. The findings revealed that 21% of the respondents below 30 years of age were ICTTs. The study also revealed that this group of respondents had not worked in other institutions prior to the employment in their current positions. The 26% of the respondent as shown in Figure 4.3 above were above 50 years of age and this comprised CLs, ULs and ICTDs.

Table 4.5: Distribution of respondents by position and age

Position/Age	Below 30yrs	30-40 yrs	41-50 yrs	Above 50years
CL	-	1	2	1
UL&DUL	-	-	1	2
ICTD	-	1	1	2
ISL	-	1	2	-
ICTT&ICTTD	4	1	-	-
TOTAL	**4**	**4**	**6**	**5**

Source: Interview data

4.3. Document Analysis

To achieve study objective four (4), the researcher collected various documents for analysis both at the university level and the library level. Table 4.5 below shows the documents collected and analyzed related to ICT as well as strategic goals of the institution.

Table 4.6: Collected Documents for Analysis

UNIVERSITY	DOCUMENTS COLLECTED
R	R Strategic Plan (2012-2015) R Library ICT Policy R ICT Security Policy
S	Strategic Plan (2009-20012) Information Security Policy e-Waste Management Policy ICT Automation Policy and Strategy Security policy or **S** Electronic Payments
T	T Library Strategic Plan (2011-2021)
U	U Library ICT Policy

Source: Interview data

4.4 Library Automation and Electronic Information Resources

It was imperative to find out whether the libraries had automated their services and also whether they had electronic resources. This in essence would imply the importance of ensuring that the CBIS which support these services and resources are protected. The services and resources included those developed in-house and those subscribed to by the libraries. The researcher also sought to know the software in use in the library in order to ascertain that there was automation regardless of the level in which it had been implemented. The researcher found it necessary to do this because the security of CBIS cannot be divorced from library automation. This would also show the type of resources, services, and ICT systems the libraries ought to protect as well as ensure integrity, availability, accountability, and confidentiality of the resources and services. The findings revealed that the selected libraries had automated several of their services. They had electronic resources that were developed in-house and others externally subscribed to from publishers. To get data about automation, electronic resources and services, data was collected through observations and interviews. The target respondents for this information included the CL, ICTT and ISL.

The findings revealed that all the target libraries had automated their services: cataloguing, circulation services, electronic charging and discharging of information resources, and OPACs which were web based. Electronic services were evident which included: e-journals, e-books and internet access. In-house electronic resources had been developed and library clients had access to these resources either through the internet or locally from the institutional intranet. The in-house resources included: Institutional Repositories (IR), exam bank and ‘maktaba’. The libraries had, therefore, established computer

laboratories or multimedia centres to facilitate research and access to these e-resources. Computers were also being used in the offices. This was illustrated by what ISLR1 said about the e-resources:

> We have a few systems and databases that are being accessed using the computer equipment…We have the library OPAC, LMS which is integrated…and we have electronic databases like the exam bank running on its own server, institutional repository which comprises data from thesis and dissertations and maktaba . The online resources which we access straight from the publisher, comprise e-books and e-journals…we are also connected to the internet. Mainly what we get from the internet especially for academic is e-journals and e-books.

The findings showed that ICTTs employed in the library as technicians for maintaining the library CBIS were aware of the e-resources the library had. This was probably because this group of staff had to work hand in hand with the librarians in their day-to-day activities that related to the use of technology. Therefore, ICTTs are involved a lot in the automation process and digitization of in-house resources. As far as the automation of library and e-resource was concerned, ICCT R1 had this to say:

> In the library, we have quite a number (e-resources) including Maktaba, IR famously known as Dspace, Koha, we have exam bank and we also have e-resources.

Evidence that the libraries had some level of automation suggested the need for preparedness to mitigate against disasters which could affect the library CBIS and cause denial of service to clients. This is because the libraries had automated their services, and had a number of their resources accessible through the internet. Libraries, therefore, need to ensure that disruption which may lead to denial of services to their clients does not happen.

4.5 Awareness and Perception of CBIS

Through interviews, the researcher sought to get views from the various respondents on their awareness and perception of what CBIS are. This was done with the understanding that for one to prepare for and mitigate against disaster for CBIS, then one needs to have an understanding of what comprises CBIS and have a positive attitude so as to take the necessary actions to protect them. The study sought to establish the respondents' opinion on what they thought computer-based information system was.

Varied views and answers were given by various respondents. Two of the UL interviewed were not willing to respond to this question. They, therefore, referred the researcher to the ICTD or the ISL. "Mukami* will help you because she is more informed than I am," said UL R2. Another, ULR1 had this to say,

"Mr. Njiraini* is in charge of the ICT department. He has details on that (CBIS) please get in touch with him."

This showed that they had little or no knowledge of what CBIS was and their responses seemed to the researcher as simply a way of avoiding the question. The ULs were well-educated since they had a Master's degree as shown in Table 4.4. It could be argued that age could have been a contributing factor as these respondents were 50 years and above, as shown in Table 4.5. It could also mean that since technology keeps on changing, these respondents had not kept themselves abreast with the happenings in the field of technology and, therefore, avoided commenting on the issue not to make a mistake that could expose their ignorance.

On the other hand, ICTDs showed understanding and awareness of CBIS, what it comprises and the role it plays in an organization. This is exemplified by what some had to say regarding CBIS:

> …this is definitely the management information system that comes with use of software and hardware and are used for processing the software. This would involve data collection, gathering of new data and processing of data to valuable information that can be used by the users. There is the difference between the IS and the IT where IS would include tools that use computer hardware and we bring in the concept IS which involves the IT and the users, the people component, reported ICTDR1.

Another respondent, ICTDR2 had this to say about CBIS:

> I would consider that to be information system, research materials, teaching materials, all manner of information including administrative information like financial, procurement all matters of management functions riding on ICT infrastructure…information plus technology…information being facilitated by use of ICT.

This group of respondents was well-educated up to Master's degree as shown in Table 4.4. Their area of specialization was in the field of information technology. In addition, half of the respondents in this group were below 50 years of age as shown in Table 4.5. These two factors could have attributed to the way in which the respondents understood the issues relating to CBIS.

Views from ICTTs indicated that this group of respondents understood what CBIS is. The ICCTR1 had the following to say concerning CBIS**;**

> I wish to think like a technician, like someone who is on the ground. These are resources that are managed by technology through computers or software management information system…resources managed by technology or through technology which allows for easy sharing, easy retrieval and storage.

Another, ICCTR4 had this to say concerning the understanding of CBIS;

> …the computers themselves, that is, the hardware, and then we have the software that is the application that runs the computer hardware…data which are part of

> the software are included because that is why we have databases.

The above responses suggest that this group of ICTDs and ICTTs had better understanding of CBIS. They elaborated this at length by giving the components of CBIS as comprising management information system, computer hardware and software, processes and data. They saw it as a system for gathering, processing, storing and enabling retrieval of information and further brought in the aspect of IT and IS. These two groups comprised of young personnel who were below 40 years of age as shown in Table 4.5.

Information systems librarians seemed not to be very sure of CBIS though they tried to explain. Majority of them saw it as use of computers in the library. This might be explained by what some ISLs had to say about CBIS.

> …possibly using computers or ICT equipment to manage the information, databases. I think in a nutshell I would explain that, says ISL R1.

> …those (systems) accessed using computers or any gadget that is electronic. Modern practices whereby we use phone or any other ICT to access information, reported ISL R3.

Surprisingly, the CLs were not aware or sure of what the CBIS was. To them it was the automation of library processes. This is illustrated by responses of some of the CL respondents. “This was infrastructure that supports the delivery of information,” explains CL R2. ”We are using Koha and we have fully automated the circulation functions,” reported CL R1. Yet, another had this to say:

> …I believe we are talking about the library online catalog that we have, we are also talking about the internet services, the e- resources, the aspect of dealing with scanning of documents, digitization, basically I think that, explains CL R3.

The responses from ISLs and CLs might be an indication that the librarians were not well-equipped with ICT knowledge and skills or they had not been trained on ICT issues and everything pertaining to ICT had been relegated to

ICCT. The researcher also noted that the training of these two groups was in the field of librarianship.

4.6 Awareness and Perception of Security for CBIS

The researcher sought to get the views of the various respondents on their understanding, awareness, and perception of what security of CBIS entailed. This was because if the people in-charge of CBIS were aware, understood, and had positive attitude towards security of CBIS, then necessary measures would be taken to ensure the systems are protected at all times. Eden and Matthews (1997) also note that staff needs to be made aware of the risks to the items in their care and what is expected of them if a disaster occurs. The contrary is true whereby, if the people in-charge of ensuring security for CBIS are not aware or do not understand what security of CBIS entails, then they will not be in a position to do much to ensure the systems are secure and ultimately taking the necessary measures to prepare and mitigate from disasters that may affect CBIS. A question on what security for computer-based information system entailed was posed to all the respondents.

The respondents showed understanding of what security entailed although this was discussed at varying levels. The ICTDs showed a better understanding of what security of CBIS entailed and described in details measures and controls that ought to be taken. All ICTDs talked about backups, rules and privileges, password, data centres and disk mirroring. However, only one mentioned about data recovery centre and indicated that in that particular institution, such a centre was in its final stages of establishment. Another mentioned security policies relating to ICT infrastructure.

The ICTTs and ISLs also talked about basic CBIS security measures such as backups, passwords, roles and privileges, disk mirroring, and personnel. Two

of the ISLs brought in the issue of N-Computing and cloud computing as they discussed security of CBIS. This showed that this group of personnel was aware of CBIS security measures though they had not implemented some of them such as N-Computing and cloud computing. The CLs on the other hand discussed CBIS at a very basic level of passwords, roles and privileges.

4.7 Threats Related to CBIS Experienced in Libraries

The study sought to find out the disasters or threats that had been experienced by the libraries prior to the study. The researcher aimed to do this from the understanding that the disasters, or threats experienced by an institution ultimately influence and determined the type of CBIS security measures to be taken. All the libraries studied had experienced various types of threats and varying levels of disasters which affected their CBIS as follows:

Theft: In this study theft was seen as taking away computing equipment without the knowledge of the librarians. Loch et al., (1992) list theft as one of computer disaster. The study concurs with this as, in all the libraries studied theft of equipment was identified as a major threat. This was especially so with computer mouse and network cables. Majority of the respondents indicated theft of computer mice. One respondent indicated loss of keyboard, another mentioned loss of a monitor, while another respondent mentioned loss of VCR and earphones.

> The only thing that was stolen was a small equipment for using CDs. Someone just came and picked a piece of equipment and went out, exclaimed ULR4.

This was echoed by the CL from the same library who lamented that the library had "lost DVD player from the multimedia centre and many of the earphones," said CLR4.

Vandalism: This is the act of illegally removing computer parts which the result into the computer malfunction**.** This was seen as a threat to CBIS in libraries. Mclntyre (1998) and Cervone (2006) note that disaster can result from an act of vandalism. The study concurs with this as 12 out of 19 respondents did cite vandalism as a major threat**.** In two of the libraries, vandalism was identified as a major problem where computers were opened and some parts removed. Physical damage was deliberately done by users where parts of the computer such as Random Access Memory (RAM) was removed or exchanged. This was so because some libraries used computers model such as Dell whose CPU cabinet was easy to open and remove essential parts In one of the libraries, ISL R1 stated:

> We're hit by a series of vandalism of hardware, any day you would find a computer has been opened, hard disk and memory card has been removed and we do not get any person…the Dell computers are easy to open and therefore, become targets for vandalism.

Computer manipulation by students: This was where software settings were changed by students without the authority of the library staff. This was a major threat to all the libraries. The study concurs with Forcht and Pierson (1994) who identified computer crime as comprising of manipulation of data, alteration of data order, holding computer hostage and hacking. The study revealed that students changed passwords, downloaded software to the library computers, hacked the systems, as well as vandalized the computers. This was noted by all the ISLs and ICTTs who saw computer manipulation by students as a major threat to their institution's CBIS. They were however quick to note that computer manipulation was done by a group of students who were taking software engineering and/or computer science courses. This was illustrated by what some of the respondents had to say:

> We have challenges related to our ICT programme here. When you train computer experts, they [students]

> come and change the configurations of the machine, open the machine and they will remove the hard disk and be left with a shell, lamented CLR3.

This was echoed by ICTTR1 who observed that:

> Another problem is the students taking software engineering, if they find a computer that is not properly secured, with Windows you can play around with it and do so many things. They change the BIOS password to the Windows and it is only that person who has that password can use the machine…the other problem is that students will come with CDs containing operating software (OS) and use it to load their own settings.

In another incident, a student was reported to have accessed his examination marks by hacking into the library CBIS using password for someone who had passed on. This would only mean that actions had not been taken by the ICT department or the Personnel office to clean the human resource database or disable the accounts once the employee died or left the organization. This created a big security threat to the system since one could compromise the systems for whatever reason and especially if the person had "bad blood" with the organization when leaving.

Actions of disgruntled employees: In a number of cases, actions of employees were seen as a major threat to the CBIS. This included the way they handled the CBIS such as the software, the hardware as well as the procedures. In one instance, employees were suspected to have stolen computing equipment from the library as well as vandalized computers. Referring to an electronic gadget that was stolen from the library, "I suspect maybe one of us must have taken it," commented ULR4.

Employees also shared passwords, causing a threat to CBIS. This was especially so at the circulation desk where a common password was given to employees working at the circulation desk. It also happened where casual employees were given passwords by their colleagues when allocated duties at

the circulation desk or had night shifts and employees on permanent basis were not available. This was explained by CLR4 who observed that:

> Currently, we are using a password at the circulation desk but almost everybody knows the password…everybody comes here (circulation desk) because of the duty roster. It becomes a risk even to other data because when I (the CL) log in, I can access cataloguing, circulation, and I am not in every time of the day. Someone may come to clear; a student may come to register any time….I log in and find my colleague using my account, I cannot tell them not to because they do not have password.

Library employees were reported to compromise the circulation system by issuing to themselves books and later discharging them from the system without returning the physical book. This, therefore, compromised the integrity of data and it was not possible to pin it to a particular person. Passwords are supposed to be confidential and strictly used by persons to access certain authorized data or information in a networked environment. The findings of the study concur with Loch et al., (1992) who identified threats to information system as comprising of intentional entry of bad data by employee, accidental and intentional destruction of data, unauthorized access to data system, inadequate physical control, among others.

At a higher level, employee's actions were also viewed to be a major security threat to critical institutional databases, because they sometimes shared passwords or even gave them out to other people. One ICTD lamented that:

> …end of last year somebody was able to hack into the student database. This was from within, it was an internal threat … internal threats are very difficult. That day, we did not have backup and the entire data for that day were lost….Sometimes lecturers give password to their children and sometimes their people in their department to enter marks….I know of a lecturer who gave the daughter password to enter marks and the daughter realized she had friends who needed to pass, lamented ICTDR1.

Change in technology: This was where new technology was introduced into the library operations. Although this was not noted by majority of the library staff who were interviewed, one of the respondents identified change in technology as a threat to security of CBIS. Nyandiere (2007) also identified increasing technology as a challenge and threat to CBIS. The respondent explained that when there is change in technology and an upgrade of the software, then data is normally lost during the upgrade or when staff use trial and error method to learn a new system. This was especially so where adequate training had not been done and, "we have been using a certain version, then when it changes it interferes with the whole thing (library operations) and loss of data," lamented CLR3. Chacha (2005) also note that insufficient training and re-skilling of end users as well as technical staff that support the system is a major challenge and threat to CBIS.

Viruses: These are computer programmes that cause harm or hamper the operation of a CBIS**.** All the target libraries reported viruses as a threat to their CBIS at varying degrees. This was seen as a major threat where the antivirus software was not regularly updated. Virus attacks were reported to have happened almost on a daily basis and especially to the computers used to access the internet. CLR2 commented that:

> Problems are related to virus and I think this is one of the greatest enemies of the kind of information we handle in an automated environment. Viruses and the regime for handling them are not consistent.

Power failure and power surges: This was a situation where electrical power went off or disrupted the system and at times the electric current flow was not consistent. Kochtanek and Joseph (2004) describe some causes of disaster as power blowout or blackout. The study findings revealed that, all the selected libraries cited power failure and power surge as a problem or threat to their

data and service delivery. In three of the libraries, the generator available to supplement or take over the electricity supply could not sustain the library for long hours. Data was reported to have been lost at the circulation desk when the power went off because the generator did not pick automatically. Only one respondent reported having clean power in the library where power supply was not an issue since backup generator was sufficient to run for days. This was illustrated by what CLR2 had to say concerning electric power:

> Another problem we need to note is the power. Power is very erratic here and you know that the moment you do not have power when you are using this technology then you are out of service.

Power surge was reported to have also caused malfunction of computing equipment such as Uninterrupted Power Supply (UPS). This caused threat to the CBIS since the likelihood of losing data when power went off was high where UPSs were not available or were malfunctioning, as observed by CLR4:

> We constantly have power failure…we have issues with UPSs especially the ones we have for each computer. Sometimes due to that (power) interruption they have a huge malfunction.

Loss of data: This was data that could not be accessed due to one reason or another. Two of the libraries studied indicated loss of data due to one thing or another. Some of this included personal data, circulation desk data on charged and discharged materials and OPAC data. Data was reported to have been lost due to either the use of flash disks that were infected by viruses or computer crash or sometimes mysteriously, where the real cause of loss of data could not be identified. One respondent indicated that it was sometimes very difficult to restore or retrieve information once it got lost. Other isolated cases mentioned as threats included the following:

Dust: In one of the selected libraries, accumulation of dust caused the computers and especially servers to malfunction and slowed down the process of information access. This was due to lack of regular cleaning. Mclntyre (1998) also identified negligence and poor maintenance as a threat to CBIS. Respondents from three of the target libraries reported that their computers were regularly dusted and dust was not a major threat to their CBIS.

Inappropriate Building: This entailed the design of the building that housed the library. One of the respondents mentioned that the size and design of the library building posed a major threat to the CBIS. This was because the building was so big and it was not possible to man all places where there were computers except in the computer labs. This made it easy to vandalize computers without being noticed. It was also noted that the ground floor of this particular library had no grills and the windows were big enough a computer to pass through. CLR1 pointed out that:

> It is easy to vandalize without being noticed and the design of the building does not deter could be thieves as it would be too easy to break into the building and steal.

Water: In this research, water was seen as flooding or leakage from pipes which affected CBIS. Water was reported to have caused malfunction of computers in one of the libraries studied. This had been caused by leakage from the top floor where computers were rained on. In the same library, it was reported to have flooded on the ground floor. Mclntyre (1998) identified floods resulting from leaking roofs, water taps and drainage pipes as causes of disaster. The researcher observed that the server room was located in the basement of the building where flooding was reported to have occurred. Further, the researcher observed that the internet gateway was located at the basement and placed on the floor where the flooding was reported to have

occurred, as shown in Plate 4.13. This could cause a security hitch, malfunction of computing equipment or loss of data if flooding ever happened again. This was confirmed by what ISLR1 reported:

> Water is also a problem. Recently, we had a serious leakage in the top floor and a few of computers were rained on and were not working or not booting. There was leakage on the ground floor but this was taken care of.

Computers should be located in places where it is not easy to flood and should not be located in the basement due to this reason. Water could also cause electrical shocks and malfunctioning of computers.

Lack of Connectivity: This referred to lack of access to information and operations of the library in a networked environment. Disconnection of power cables or network cables was reported to have caused denial of services and sometimes loss of data. This happened where the server had been disconnected from power supply or the network and therefore, switching off the server. This caused denial of service to the clients and sometimes loss of data. In addition, power overload by users was also reported where more electronic gadgets were plugged into the power outlet causing overload to the power sockets. This made computers to malfunction. ISLR1 commenting on electricity overload noted that the library had "encountered issues with some equipment especially with fuse exploding and burning due to overloading the system with power." Further, it was reported that the bandwidth was sometimes a challenge causing delays to service delivery due to slow connections.

4.7.1 Preparedness for Disaster

The study sought to find out whether the libraries or the institutions perceived themselves as adequately prepared for disaster that might affect CBIS or not. The information was sought from ICTDs, ISLs and ICTTs. This was done by

posing a question regarding their opinion on whether they thought they were prepared for disaster that may affect CBIS in the library.

Though the researcher got from the respondents a 'yes' and 'no' answer followed with an explanation, this was aimed at finding out what measures had been put in place and challenges faced by persons responsible for ensuring that the CBIS was up and running. Although it was not possible to be fully prepared for a disaster or be in a position to mitigate all the disasters which could affect the CBIS, the respondents indicated various levels of preparedness and gave reasons as to why they thought they were prepared or not fully prepared. Commenting on preparedness, ISLR1 pointed out that: "It was partially 'yes' and 'no', there is no system in the world that is secure, you only do the much you can humanly do but make sure if you go down you won't remain down but you are able to come up."

The respondents gave various reasons as to why they thought they were prepared which included the following:

i. Measures had been taken to ensure library operations were sustained under all circumstances.
ii. Data was not internally stored since library servers were located outside the library.
iii. Good fire fighting facilities had been put in place.
iv. The management's willingness to support ICT department to develop ICT policies, disaster recovery planning, carry on trainings on ICT disaster and establishment of an offsite disaster recovery sites.

The respondents thought they were not fully prepared for disaster and gave the following reasons:

i. The field of information security is dynamic and one may never know which new routine will come up later and compromise security.
ii. No system is fully secure but one only needs to do what one can to ensure if the systems are affected they can be restored to normalcy.
iii. All measures to ensure the library CBIS could go back to where it was in case of a disaster had not been exhausted since the libraries were still growing.

From the information gathered, it was evident that preparing for and mitigating against disaster for CBIS was itself a challenge and one could not be in a position to tell whether they had adequately prepared or mitigated against disaster at any one particular time due to the dynamic nature of technology.

4.8 Measures Taken to Prepare and Mitigate Disaster for CBIS

The researcher assessed measures that the institutions and target libraries had put in place to prepare for and mitigate against disaster that could affect CBIS. To do this, the researcher explored the issues which indicated preparedness or lack of it to mitigate disaster that could affect CBIS. This was achieved by collecting data through interviews, observations, and document analysis. The data collected indicated high level of awareness of measures that should be taken. Majority of the respondents outlined the measures that needed to be taken whether they were in place or not. These were categorized as follows:

i. Physical measures
ii. Procedural measures
iii. Technical measures

4.8.1 Physical Measures

These were measures that were observable and the researcher identified during the study. Physical measures had been put in place in all the libraries that were studied. These included the following:

i. To curb vandalism, one of the libraries studied had chained the cables together using steel wire. This was meant to prevent computers from being opened as well as prevent computer peripherals such as mice and keyboard from being stolen. In addition, the library was big and it was a challenge to place security guards in all areas where computers were located. This was confirmed through observation as shown in Plate 4.1 and Plate 4.2. below. This was done due to the fact that vandalism and theft of computer parts had been identified as threats to CBIS.

Plate 4.1: Hardened wire used to tie the CPU cabinet at the back in one of the libraries. ***Source: Observation.***

Plate 4.2: Hardened wire used to tie cables together in one of the libraries.

Source: Observation.

ii. Other libraries used 'tiebacks" also referred to as clips, where cables were tied tightly at the back. This was used to discourage or prevent theft of power cables, network cables, keyboards and mice. This was observed as illustrated by Plate 4.3, Plate 4.4 and Plate 4.5 below:

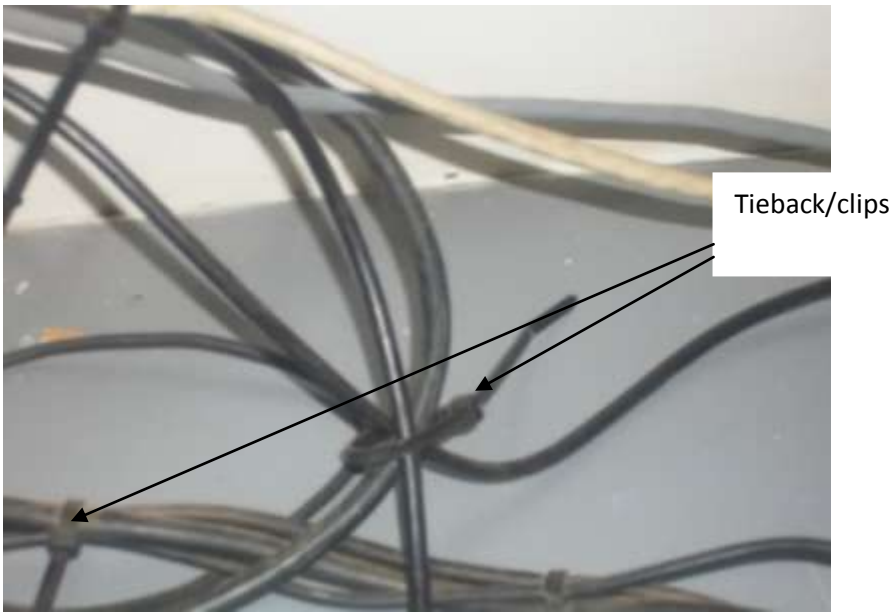

Plate 4.3: Tie back/clip used to tie cables together in one of the libraries.

Source: Observation.

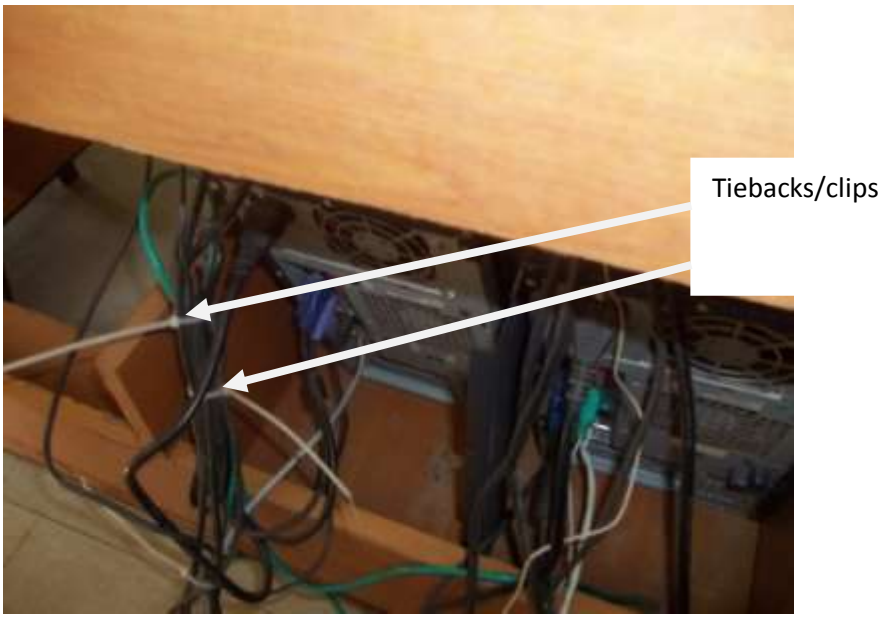

Plate 4.4: Tiebacks/clips used to tie cables together in another library.
Source: Observation.

Plate 4.5: Tiebacks/clips used to tie peripherals together in yet another library. ***Source: Observation.***

iii. In another library, lock and key (padlock) had been used to lock the CPU cabinet to prevent anyone from removing parts of the computer or tampering with the inside of the computer. This was as shown in Plate 4.6 below as observed by the researcher in one of the libraries.

Plate 4.6: A padlock was used to lock the CPU cabinet in one of the libraries

Source: Observation.

Lock and key were also used to curb theft of computing equipment in offices, the server rooms, cabinets and computer labs in the libraries. In addition to the use of lock and key, only a few respondents indicated use of control measures such as record keeping and centralized place for storing keys as a measure to enhance security of CBIS. In one instance, ICTDR4 had this to say on security of hardware:

> On the level of hardware we ask people to be cautious of their environments…keep them under physical lock and key that at least ensures you have solved the loss of hardware, locking of offices, locking of our cabinets where equipments are stored.

Although use of lock and key was noted in only one library, this was a measure that another library was contemplating taking except that it took too long to deliver padlocks and, therefore, the library had to improvise by using hardened wire to tie the CPUs cabinets, peripherals and cables together as shown in Plate 4.1 and Plate 4.2.

iv. Tagging (engraving codes) on the equipment was another method used to deter would be vandals or thieves. Marking or tagging the peripheral

equipment that were targeted for theft or vandalism had been used in areas that were easy to identify or see to discourage theft of the peripheral equipment such as mice, keyboard, UPS among others. Plate 4.7 below illustrates this which was captured through observation.

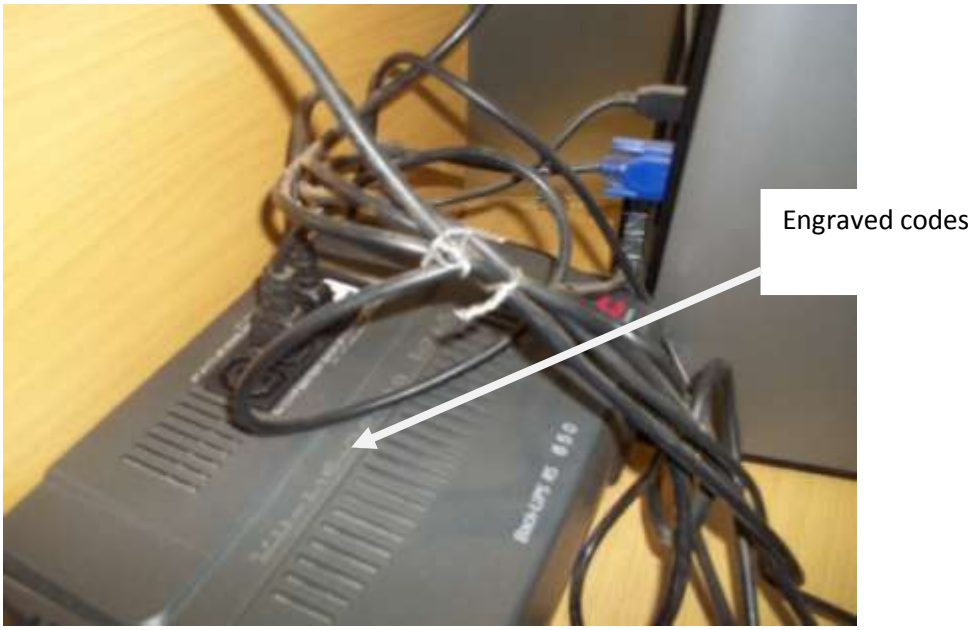

Plate 4.7: Engraved codes on the UPS. ***Source: Observation.***

v. Putting magnetic strips. One of the libraries studied used tagging (engraving codes) as well as putting magnetic strips in some "hidden" parts of the equipment to ensure any equipment leaving the library was detected by the electronic security system at the exit door. The magnetic strips were not observed by the researcher as the respondent felt it was a breach of security and confidentiality to seek such information. Allowing the researcher to observe areas where the magnetic strips had been put was seen as a threat to security itself.

vi. Use of closed-circuit televisions (CCTVs). In one of the libraries studied, CCTVs were used to monitor the happenings at the OPAC areas to prevent vandalism of computers. They were installed in the essential areas where theft had been reported to have taken place. This was done at each floor where the

computers were located especially the OPAC computers which were highly targeted for vandalism, theft, and unauthorized downloading of software. ISLR1 noted that:

> on each floor we have 18 computers for OPAC, these are the ones mainly targeted for vandalism and we have therefore put in place surveillance cameras to monitor the happening in these areas.

Although the surveillance cameras had been put in place as a measure to monitor the happenings and probably catch those who vandalized the computers, the researcher noted that the surveillance control room where monitoring was meant to occur was in most the times left without anyone to check what was happening in these areas.

vii. **Personnel**. Securing CBIS using personnel was done at two levels:

a) **Use of the library staff**. Library staff were used to man various places where computers used for research purposes were concentrated. Other personnel manned computer labs in the library. They played a double role as reference persons in the library as well as in surveillance, in order to deter vandalism in these areas. Library staff had also been sensitized to ensure they are vigilant on the happenings within the library as well as ensuring they protected their passwords. ISLs and ICTTs from three of the target libraries mentioned that they held staff responsible for computers in the library as well as for the ones they used in their offices. This was done to ensure protection of the hardware, applications, and data within these computers. Commenting about the high level of vandalism in one of the libraries, the ISLR1 mentioned that they had:

> Alerted people at each floor and we told them if anything is removed they will be responsible. The security guards, cleaners, librarians, everybody was told to be vigilant. …there is a system where

> everybody is made accountable of what is lost whether a guard or a library staff.

This seemed to have worked because two libraries reported to have charged security companies for computers that had been stolen from them. Security guards were charged because a monitor was stolen from the library and the library staff felt that a monitor was big enough to have been noticed at the exit door which the guards manned. Library staffs were used to control installation of software by users and staff manning the computer laboratories ensured that users did not install software into the library computers. They also ensured that theft and vandalism did not take place in the computer laboratories.

Through observation, it was noted that the majority of the staff manning computer laboratories in the target libraries, did not do much to check what the users did. They were located at a corner and the only thing they were concerned with most of the times was clocking in of the users, although the users did this voluntarily. Laboratory assistants in one particular library were observed to be on Facebook or listening to music most of the times and never went round checking what the users did.

b). **Security guards.** Two of the libraries (one public and one private), had security guards who were employees of the institutions but not trained librarians. In other two libraries (one public and one private), guards from security companies were used. In all four libraries, the guards were used to man the exit door and to check what each person leaving the library was carrying. The guards also made rounds in the library to check any person who could be vandalizing computers. This was used as a way of deterring users from vandalizing computers or even stealing them. The ICTTR1 had this to say:

> We have been seeing our security guards walk around the floors especially during the day when the traffic is high. They always go checking whether someone is doing something funny or something that one is not supposed to be doing.

Security guards were also given the task of ensuring security around the building especially at night as a way of preventing thieves from breaking into the building or even users stealing and passing computing equipment from the library through the windows. Fitzgerald and Dennis (2002) concur with this as they note that preventive controls are those which mitigate or stop a person from acting criminally or which prevent an event from occurring such as use of password, guard and security lock.

viii. **Security lights**. One respondent mentioned good security lighting at night outside the building as a method that the library had used to deter theft from the library.

4.8.2 Procedural Measures

In this section, the researcher provides the procedural measures that the target libraries had taken to prepare and mitigate disaster that could affect their CBIS. These measures were as follows:

i. **Clocking/recording:** In all the target libraries, where computers had been set aside for research purposes or computer laboratories had been set, users were required to register in a book and also show their identification cards. This was done in a bid to ensure that only authorized persons used the computers. It was also meant to act as a point of reference if anything went wrong to any computer in the laboratory. Through observation, the researcher, however, noted that the library personnel in most cases did not confirm that users recorded the right details but were instead left to fill in detail on their

own. Anyone could, therefore, have entered incorrect details. In that case, if anything bad happened, it would be very hard to track down the culprit.

ii. Training and sensitization of employees and users in general. Three of the target libraries indicated that they sensitized their employees on issues related to security of their CBIS in different ways. One institution had a well-structured programme of training as a form of sensitization, while others mentioned sensitization of staff, but had no clear method of doing it. This was as observed by ICTDR1 who said: "Over the last two years we have been conducting information security sensitization to our staff."

The same ICTDR1 reported that the sensitization focused on password use among other issues related to security of CBIS. In another library, training and sensitization was normally done through workshops, seminars, and brochures. New staff and students were taken through a process of training where they were trained on when and how they were expected to use the computer system. This entailed going through rules put in place and sign-in procedures. Training was done as need arose and especially when new systems were introduced.

In one instance, ICTTR4 mentioned: "there was staff sensitization about where they are supposed to be and where they are not supposed to be."This was in relation to authority to access certain places where ICT databases resided such as server rooms. Sensitization was also done to ensure staffs were responsible for their machines and property in the library. Other measures observed in all the libraries were notices hanged in computer labs, on desks where computers for research purposes were located. These entailed the do's and dont's on the use of computers.

iii. **Anti-virus**: In all the libraries, use of anti-virus software was mentioned as one form of ensuring security of CBIS. However, the type of anti-virus used and the form of upgrading differed from one library to another. Majority of the respondents indicated use of co-operate license which was updated automatically.

iv. **Firewalls:** These are software used to protect outsiders from accessing information held in an organization. Use of firewall to protect institution's computer network from external threats was noted by ICTDs, ICCTs and ISLs. This was especially so due to the use of internet in the targeted institutions studied. Firewall was used to prevent hackers and crackers from accessing the institutions' network. To this effect, the ICTDR1 reported:

> The other measure we put in place is to ensure our systems and data that we have is also protected from outside access through the use of firewalls and therefore, we have a perimeter firewall which is a CISCO 5520.

This was echoed by ISLR1 who indicated use of firewall as a way of preventing hackers from accessing the library system. The ISLR1 had this to say:

> We depend mainly on university firewall system in terms of securing what we have here …as far as library is concerned those databases we think are prone to hacking are only accessed through our LAN such as exam data bank.

v. **CBIS security policies.** Loch et al., (1992) note that the ultimate aim of any computer policy must be to protect the integrity, availability, and confidentiality of the electronic data held within the system. The study findings revealed that only one institution mentioned use of computer security policy as a measure used to ensure security for CBIS. The ICTD in this

institution felt that the several ICT related policies that had been developed played a major role in security of their CBIS.

CBIS security policies played a major role in ensuring security as they provided a framework through which directions were outlined on what should be done, by whom, and when. The researcher observed that several CBIS security policies had been implemented, chief among them being information security policy and electronic payment security policy.

vi. **Redundancy**: In all the target libraries, replication of data in various places and in various forms was viewed as a method of ensuring that the data and databases were safe or if anything happened, it would be possible to get back the data and databases. This was done through disk mirroring of servers and sometimes backup servers. This concurs with Chow and Ha (2009) who saw data, documents, data files and mail backup as a way of providing redundancy to facilitate recovery after a disruption, corruption or disaster has occurred.

4.8.3 Technical Measures

In this section, the researcher provides the technical measures which the target libraries had put in place to prepare for and mitigate against disaster. They included the following:

i. Username and password: This was reported by all the respondents interviewed. It was seen as the most basic form used to ensure that only authorized persons had access to data and databases. However, procedures and process of creating user accounts and password differed. The guidelines on management of these passwords also differed among the institutions studied. CLR1 mentioned use of username and passwords for the circulation module, and noted that even those who worked in shifts and especially on Saturdays

were also given passwords. However, the CLR1 was quick to note that the passwords were shared where:

> Everybody at the circulation desk uses these two passwords…everybody comes here (circulation desk) because of duty roster.

In another library, passwords were used to ensure only authorized persons had access to the databases. The ICTTR4 observed:

> They were using the passwords so that somebody cannot be able to access the information unauthorized because that is one of the issues that cause insecurity… people who are supposed to interact with the system have been given credentials, that is , they have been given user names and passwords.

Strong passwords were deemed necessary to prevent people from guessing. ISLR1 reported use of strong passwords which were alphanumeric and they were changed every two weeks. These were the passwords used to access the server. Only three staff members had access to these passwords, which were not written down anywhere. The passwords were only to be given to any other person with permission from higher authority.

ii. Backups. Backup is a copy of the original item taken and kept in case anything happened to the original item. Backups were done at different levels as indicated below:

a) Data/database backup

Chow and Ha (2009) note data backups as major component of disaster control planning and a detailed plan of backing up was seen as vital that must cover issues of frequency, type and location. All the respondents mentioned backup as a major form of ensuring security for data and databases. There were, however, differences among the respondents in areas such as forms of backup, storage of backup, frequency of backup, testing, and policy or guidelines pertaining to backups. This was illustrated by what some

respondents said concerning backup: “We are encouraging both at personal level and institutional level to have backups,” noted one ICTDR4. Another ICTDR2 noted “that in their institution, automatic backups were done on a weekly basis and on a separate backup server”. The researcher noted that this was such a long time (a week) for a big and busy institution. Having backups on a weekly basis meant that there was likelihood of losing data for one whole week if anything happened, which was massive loss of information for an institution like a university. In one library, the ISLR1 mentioned that the library backed up the information every day:

> Backup is supposed to happen either every morning or every evening. Every morning we backup data of the previous day or every evening we backup data of that day, ISLR1 said.

Backup servers and backup machines were used to store data where some were remotely located as a way of ensuring resumption of the CBIS in case of a disaster. In another institution, the ICTDR4 mentioned backing up on the hard disks three times a week. Thus in each day, a different hard disk was used and an incremental backup was taken for those particular days.

Offsite backup was also another method used to ensure preparedness for and mitigation against a disaster. This was mainly done in satellite campuses though one institution had their backup servers in one of the companies within the university, as well as in a different building within the main campus. In another institution, office documents were backed up at the departmental level using hard disks:

> …backups are essential, the information resident within the department we encourage them (departments) to ensure they keep them safe in a secure external hard disk, mentioned ICTDR3.

Other methods used included use of external drive to do automatic backups, and keeping a dump copy from the servers' desktop in the ISL's PC. Only one institution talked of data recovery server which was located in the primary data centre waiting to be moved to a data recovery centre which was being established in one of the institutional campuses.

Testing of backups:

Testing of backups was mentioned as a way of ensuring that if anything happened to data or databases, then the backups could be used to resurrect the malfunctioning system. Testing of backup varied from one library to another. Some had a biweekly backup though ICTDR4 felt that this should be a daily affair. No library had a written policy on backup testing or scheduled backup plan though some felt that this should be put in place to ensure regular backup.*"*We have been testing our backups and this is an exercise done twice a week but the frequency should be daily", observed ICTDR4.

b. Power backup

In all the libraries studied, generators and UPS were used for power backup. Though this was the case, not all libraries indicated that the generators could support the activities of the library for long hours. Only two libraries were confident that power was not a problem since the generator could run for a long time.

> The library has clean power all the time and the generator can run for days, weeks by diesel. They (maintenance department) always make sure they have enough diesel if power shortage is expected, claimed ISLR1.

UPS were also indicated as a method of ensuring power backup. This was especially so to ensure proper shutting down of the system and continued service on the side of the server. It was reported that some UPS could take up

to 4 hours which was long enough when there was power blackout. “UPS are used as power backups and UPS supporting the servers can take up to 4 hours”, noted ICTDR4.

c). Connectivity backup

As a way of ensuring availability of internet service, different companies and methods were used to ensure enough bandwidth and continuous internet connectivity. Three of the universities studied, reported use of different ISPs as well as use of Kenya Education Network (KENET) as an approach used to ensure continuous and adequate internet connectivity. In the institution R, clustering of the network was mentioned as one of the methods used to ensure internet services to the clients:

> Our network is clustered whereby even if the fiber optic is cut or network equipment destroyed in one area it will only affect that one cluster but will not affect the whole institution, noted ICTDR1.

To ensure continuous service delivery, institutions that were studied used a variety of different modes of internet connectivity, including fiber optic networks, wireless technology and radio link.

iii. Use of rights and privileges: In a networked environment, users of have different types of data or database that they are authorized to access. To ensure access to these different types of data in the network, rights and privileges are normally used to control access to unauthorized data. This is normally done depending on the functions or duties of each different person using the data or databases and applications in the network. All the libraries studied used rights and privileges to control access to the applications and databases in their custody. The system administrator in one of the libraries studied was charged with the duty of creating accounts, giving passwords, rights and privileges to the clients.

iv. Authorization and access control: It was observed that in all the target libraries there were measures put in place to ensure control of who entered or used the computers in the libraries This was especially so to the computer labs and server rooms. Server rooms had controlled access and the keys were kept by only a few authorized persons. There was also control of use of computers in offices where staff were discouraged from using computers which belonged to other members of staff.

v. Magnetizing: In one of the libraries, the ISLR1 mentioned that they used magnetic strips to tag computer equipment so that in case anybody tried to steal a computer gadget, the electronic security system would detect this gadget at the exit door. The ISLR1 mentioned that this had worked well and a number of users had been caught leaving with mice.

Others measures mentioned included the following:

vi. Budget: Although budgeting was mentioned as one of the major challenges, ICTDR1 reported that ICT directorate had enough budget to support the day to day running of the ICT infrastructure. This was especially so with the recurrent budget:

> One thing is that we have a good ICT budget. 200 million per annum expandable so we can easily be able to buy other computers within a short time in case of theft, so the business will continue, observes ICTDR1.

vii. Insurance cover: Only one institution cited insurance cover as a CBIS security measure. Insurance cover had been taken against loss of hardware. This, therefore, meant that the institution was aware that loss to the CBIS remained a challenge and measures had been taken to ensure that at least part of it (the hardware) was replaceable in case it was lost. Insurance cover had been taken as a way to cover for theft or loss of equipment through break-ins.

Some of the respondents had this to say concerning insurance. **"**There is insurance cover whereby if we lost equipment we will get money to buy the equipment," observed ICTDR1. "I understand the library equipment is insured 100%...if we lost everything we get it back," echoed ISLR1.

Incidentally, the ICTDR1 seemed not to have much detail about the form of insurance. The insurance cover was arranged and run by finance department where details of the computers were given to finance department by the ICT department. This was as reported by the ICTDR1 when asked more about the type of insurance taken.

viii. Encryption: One respondent touched on encryption software as a method used to secure CBIS in the institution. This was used to mark the gadgets to deter theft. Software had been downloaded, customized and used for encryption starting with laptops which were the main targets for theft:

> We have downloaded software and customized it for use for encryption and we have started with laptops because we have realized over the last few years we have been losing a lot of laptops, observed ICTDR2.

ix. Warranty: All ICCTs and ISLs indicated that one year warranty was normally arranged with the suppliers or vendors of the hardware computing equipment**.** This was whereby the suppliers of computing equipment had an agreement to maintain it for one year. However, the researcher noted that the institutions did not renew the maintenance agreement after the one year warranty and the ICT department was mandated to handle the day-to-day maintenance work of the computing equipment.

x. Software: Two of the libraries studied used software to ensure that their CBIS were not compromised. This was especially so with the server operating software. In this case, it was reported that there were few problems of viruses

attacking the server although for the terminals or stations running on windows virus attacks were reported to be high. Software was also used to authenticate users in the system to ensure that only authorized users of the system logged into the system:

> … servers run on LINUX platform. A Linux platform is very hard to hit with a virus and we have software to allow one to log in, reported ICTTR4.

xi. Disabling drivers: Another method used was to ensure the drivers were not active. This was used to prevent installation of software by the users. The ICTTR1 reported this as a measure used to curb this menace from students. This, therefore, made it hard to install other software into the library CBIS as unauthorized software could compromise the integrity of the existing databases.

4.8.4 Awareness of CBIS security Measures

The success of any venture depends first on the awareness of what it entails. To ensure disaster preparedness and mitigation for CBIS was dependent first on the awareness of what should be done. The researcher assessed whether the respondents' were aware of measures used to secure CBIS regardless of whether the measures were in place or not. It was evident that almost all respondents had some level of awareness of what needed to be done. All the ICTDs and all the ICCTs interviewed showed high level of awareness of the measures that should be put in place to prepare for and mitigate disaster. This was shown by the level of detail in which measures were explained. They, however, explained that they had not implemented most of the measures discussed and gave a number of reasons why they had not done so. They talked of what they hoped to do in future thus demonstrating their awareness and knowledge of CBIS security.

The ISLs and majority of CLs were only aware of the very basic measures like backup, passwords, roles and privileges, use of guards, and access control to computer rooms or labs. For the CLs the researcher noted they did not distinguish between uses of passwords and rights and privileges and they discussed this as one and the same thing.

The ULs seemed to be less informed than other respondents on issues relating to technology. This group of respondents avoided answering questions about CBIS security. The researcher's observation was that this group of respondents was somehow advanced in age as shown in Table 4.5. The training was also in the field of librarianship which could have been a contributing factor as well. Issues pertaining to ICT were referred to the ICTD, ISL or the ICTT.

Incidentally, the group of respondents that appeared to be less informed on issues related to computer technology were the same people who "feared" technology and could not allow the researcher to audio-record them during the interview.

4.9 Indicators of Unpreparedness for Disaster Related to CBIS

The researcher collected data on issues that assessed lack of disaster preparedness and mitigation for CBIS. Despite the high level of awareness of CBIS security measures among most of the respondents, the researcher observed a number of security risks as indicated below.

i. **Reckless placing and exposure of the network and electrical cables**. This is as shown by Plates 4.8 and 4.9 taken from various libraries

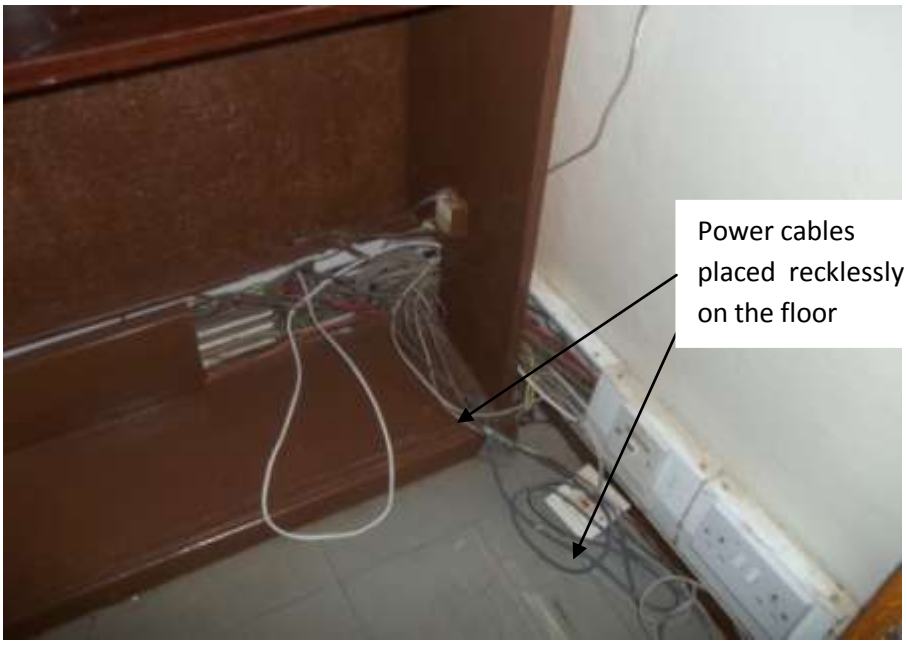

Plate 4.8: Power cables and network cables placed recklessly on the floor. ***Source: Observation.***

Plate 4.9: Power cables, network cables and multi plug all placed recklessly on the floor. ***Source: Observation.***

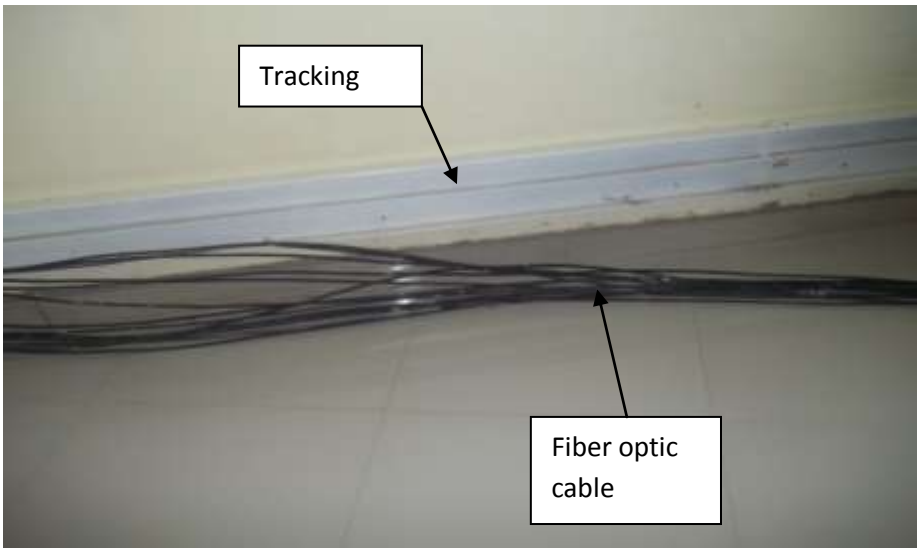

Plate 4.10: Fiber Optic cables placed on the floor yet the tracking is provided for to hold the cables together. ***Source: Observation.***

In three of the libraries studied, the researcher observed active electric cables lying on the floor and active, uninsulated electric cables hanging dangerously from the wall. This could lead to electrical shocks, or damage by water and especially during cleaning. Network cables could easily be disconnected denying service to users of the network. It could also encourage vandalism as it was very easy to unplug the cables.

ii. Location of server rooms, servers, gateways, switches, and other internetworking devices

There was no library that had a purposely designated room to keep essential computing equipment such as servers. The "server room" for those libraries that had a designated room for servers did not meet the minimum server room specifications such as; air condition, not being in the basement or ground floor, controlled access and free from dust. In one of the institutions studied, the "server room" doubled as a store and a room to keep the server as shown in Plate 4.11. The researcher observed that the server was placed on the floor and had accumulated dust. There was no ventilation, and no cooling system. The cooling fun which was available was not functional and was of a type that was not recommended for use in a server room because when in use dust was

blown to the server causing malfunction. These were unacceptable conditions for a server room because dust and heat alone could cause the server to run inefficiently or to break down. Air conditioning systems are recommended in server rooms. Servers are to be placed on a raised floor to protect them from water and dust. The 'server room' was also accessible to several people with no record to track who entered, the time they entered, and what they did in the room. This was a security breach because one cannot trust people all the time and, therefore, the server room should have controlled access.

Plate 4.11: Server room which doubled as a store where server was placed on the floor. ***Source: Observation.***

In another library, the ISL office doubled as the "server room" and the ICTT personnel's office. Traffic to this room was not controlled and the "server" was kept in this room together with hard disks that had essential backup of the library data. This was as observed by the researcher as shown in Plate 4.12:

Plate 4.12: Server room which doubled as ICTT's office in one of the libraries. ***Source: Observation.***

In another library, the main network gateway was placed on the floor and housed in a room in the basement of the library building. This was as shown in Plates 4.13. The network cables and power cables lay on the floor unprotected. The server room though not equipped was also located in the basement as shown in Plate 4.14. Ideally, basement is not the recommended location for server room because they are prone to flooding. In fact, one respondent mentioned during data collection session that there had been a case of flooding in that particular building. In the same library, the researcher observed that switches were located along the corridors where there was high traffic making them prone to vandalism and damage by library users.

Plate 4.13: Gateway located in the basement and placed on the floor

Source: Observation.

Plate 4.14: Server room located in the basement in one of the library buildings ***Source: Observation.***

iii. Location of backup servers and data backups devices

In three of the target libraries, backup servers were kept in the same building with the rest of the computing equipment holding the original data. This is not a recommended scenario since in case of a disaster - such as if a complete destruction of the building occurred, then the backups would also be destroyed. Backup servers and data backup devices are required to be kept in a different location away from the originals.

iv. Power backups, electric filters

The researcher assessed the measures taken to prevent data loss due to electric spikes or power failure. Results showed that none of the libraries had installed electric filters to their computers. Generators were used as power backups, but only one respondent reported that the generators picked up automatically if power went off. Respondents from the three other libraries studied indicated that they were supported by generators as power backup but these generators did not start automatically when power went off. It was also reported that many of the UPS provided for individual computers to allow saving of data when power went off were malfunctional.

v. Lack of policies, training programme and disaster recovery plans

In all the target libraries, there were no policies, training programmes or disaster management plans that had been approved by the management. In this case, if a disaster happened no one would take the responsibility and there were no guidelines on who, what and how to go about the disaster. It was only in one institution where information system security plan had been developed as an institutional wide policy. Chow and Ha (2009) realize the need for an effective data backup policies as well as policies and programmes addressing training for organization employees on disaster prevention and recovery.

vi. **Lack of co-operation between the library and the ICT directorate**

If and when a disaster strikes, where a disaster recovery team exists, it would have the mandate to ensure things return to normalcy. Even where this team does not exist, various people must work together to ensure the library systems are up and running. Therefore, cooperation between various departments is very crucial and especially the ICT directorate whose expertise would be needed when it came to CBIS. Results from this study showed that in one of the libraries, the library department and the ICT directorate did not always work together in harmony, but viewed each other as competitors rather than playing complementary roles. Lack of cooperation between these two departments could make it difficult for the institution to recover from a disaster affecting its library CBIS. Eden and Matthews (1997) concur with this as they point out the importance of liaison between libraries, IT personnel, internal computing department and service providers in establishing security and recovery requirements, temporary service and access arrangements for CBIS as a way of preparing for disaster.

4.10 Personnel Involved in Disaster Preparedness and Mitigation for CBIS

The researcher sought to find out persons involved in ensuring security of library CBIS, focusing mainly on their skills, knowledge, training, and on inter departmental cooperation. It was also important to check whether there existed disaster recovery team(s) in the institutions. If the disaster recovery team existed, the researcher was interested in establishing the composition of the disaster recovery teams in relation to departmental representation, training, and relevant skills.

The findings were grouped into various subthemes as follows:

i. Role of management in disaster preparedness and disaster mitigation for CBIS.

ii. Training of staff on ICT related issues as well as on disaster management.

iii. Education, training and skills of personnel responsible for CBIS.

iv. Composition of disaster recovery teams.

v. Personnel involved in development of ICT policies, plans, and programmes.

4.10.1 Role of Management in Disaster Preparedness and Disaster Mitigation for CBIS

The top management determines the direction the university ICT infrastructure takes. They are involved in creating awareness of what business continuity for CBIS entails, staffing, financing of the ICT infrastructure, as well as in development of ICT-related policies, plans and programmes. Loch et al., (1992) concur as they note that protecting a corporation's information system and data warrants management attention.

The study found that in three of the institutions studied, top management did not provide enough or required support to the ICT directorate. This was in regard to the ICT directorate needs such as staffing, ICT infrastructural needs, skills requirement. Top management also lacked awareness on various issues concerning the ICT directorate such as the functions of the ICT director. The findings concur with Eden and Matthews (1997) who note that disaster management seem to be one of those managerial activities which are put off until a later date. In one instance, the ICTD mentioned lack of awareness by the top management regarding what was required in relation to disaster management for CBIS as well as staffing of the ICT directorate at the university. Also, in relation to involvement of top management, another ICTDR1 claimed: "the management will not be aware of what entails the job description of an ICT director so when they are hiring they will hire an ICT D

without a job description. The ICTD had therefore, to draw the job description long after the hiring had been done since "the University management may not be able to do this (write job description) because they are not aware of the duties and responsibilities of the ICTD,"ICTDR1 continued to say.

In all the target institutions, ICTDs, ICCTs and ISLs reported that the management was very supportive in budgetary allocation:

> at least in terms of budgetary support, we are seeing the university management moving closer and closer towards supporting ICT infrastructure, systems, and service development. We are receiving a lot of championship from the Vice Chancellor, the council, ICTDR1 noted.

This was echoed by ISLR3 who reported that:

> Management is very supportive, for example, I am sure a lot of money was used in the tagging process, the management has been involved in whatever system the library requests, they ensure they purchase…if the management does not support this you are headed nowhere.

Although the top management was in support of development of the ICT infrastructure, all ICTDs noted that support from management was dependent on the advice given by the ICT directorate. ICTDR4 said:

> the top management will make quality decisions depending on the quality of advice from the ICT Directorate…it is ICT directorate that should do proper planning and advise management, this is what we require….

Another, ICTDR2 had this to say commenting on the support by the top management:

> it all depends on us, on our requirements, and this is what we will communicate to the management. The management is normally supportive.

4.10.2 Training of Staff.

Training of staff and students on how to take care of the ICT systems is critical in ensuring the systems are effective and efficiently used. The

researcher, therefore, investigated whether there was any ICT-related training carried out in these universities. Three of the institutions studied did not have any structured training programme on CBIS. Trainings were carried out haphazardly through workshops, conferences and seminars. In the libraries, the do's and dont's on the use of CBIS were mentioned during the induction session for the new staff. Only one institution reported to have carried out structured training in the institution and also saw the developed policies as a basis for security sensitization seminars:

> …we must conduct sensitization sessions. It is scheduled every year but it is planned to cover the complexity of the University … it is currently through seminars and ICT related policies are the basis of the information security sensitization seminars, reported ICTDR2

In another institution, training was carried out through workshops, seminars or conferences as needs arose though this was dependent on the availability of funds.

4.10. 3 Education, Training and Skills of Personnel Involved in CBIS Security

The education level, training, and experience in most cases influence the way an organization or a department runs. The researcher sought to find out these aspects with regard to the personnel involved directly or indirectly in ensuring security of CBIS in the library. These included the UL, the ICTD, the ISL and the ICTT.

The findings revealed that all the ULs interviewed had a Masters degree and one DUL had a PhD as shown in Table 4.4 (Page 55). Therefore, this group of respondents was well- educated and had gained experience from a number of institutions where they had previously worked. However, one respondent had worked in the respective library for more than 15 years and had not worked in any other library. Though well-educated, the researcher noted that the

education for this group of respondents was not in the field of ICT but in the field of librarianship whereby the second degree had been obtained more than 15 years in all the cases. Therefore, this group of personnel seemed to have only the basic knowledge and skills in ICT issues.

All ICTDs were well-educated and all of them had a Masters degree as shown in Table 4.4 (Page 55). Although this was the case, one ICTD had a Masters degree in theology while the others had the Masters degree in ICT-related fields. Three members of this group of respondents had been trained on ICT security issues. It was, therefore, evident that the ICTDs who were well-educated in the ICT field had skills, knowledge and experience on issues related to ICT security. This was well-demonstrated by the confidence they portrayed in tackling the questions during the interviews and the detailed discussions in responding to questions. Lack of education, skills, and experience on ICT-related issues might have hampered proper direction and smooth running of the ICT-related issues in the particular university where the ICTD lacked education and training in ICT-related fields. It was no wonder that the ICT issues were fragmented and handled at the departmental levels. There was evidence of lack of policies and proper measures to ensure disaster preparedness and mitigation for CBIS in this particular University. The ICTD relied on his junior staff for direction and it was reported that sometimes there was sabotage due to lack of understanding. This was also evidenced by the fact that the ICTD declined to be interviewed alone and had to be accompanied by one of the junior staff during the interview. Incidentally, the junior staff seemed to dominate the interview session which was meant for the ICTD.

All the ICTT had first degrees in ICT related fields from local universities. Three of them had not worked in other institutions and therefore, the respective libraries were their first places of work. They, therefore, lacked necessary experience and skills that could have been gained from experience either in their current job or elsewhere but rather used the knowledge gained from class (during training). One of the ICTT had worked in a similar position in a library in another institution but had only worked for 7 months in the current library. This meant that the impact of his skills and knowledge was not quite much as one ICTD had earlier noted that one needs at least 6 months to get along with a new system. In one of the libraries, the ICTT had been hired on contract basis and this hindered his operations since he was not allowed to access some crucial documents relating to security of CBIS. Commenting on this kind of engagement he had this to say:

> As a casual (employee) there is only so much we are entitled to, and some of these documents cannot be handed to us because there are respective people who are supposed to handle those documents. It will be bleach of rules and regulations if we get access to some of these things (policy documents), reported ICTTR1 commenting on what the role of ICTT entailed.

The ISLs had education levels ranging from Diploma to PhD as shown in Table 4.4 (Page 55). All of them had training in the field of librarianship and two were hired as librarians and later seconded to man the ICT section due to their interest in ICT-related issues in the library but not because of their education level in ICT or training in ICT field. In one case, the ISL was hired as an ISL but not due to education, skills or knowledge in ICT but because the staff had some background knowledge in ICT during the time of hiring as it was reported by the deputy university librarian during the interview. This, therefore, meant that these personnel were quite limited in the direction and guidance on ICT-related issues although the libraries looked upon them for guidance. Coupled with this is the fact that the ICTT worked under the ISL who

were not in a better position to guide ICTT on issues related to ICT neither was the UL. This is well-demonstrated by what one UL had to say:

> … Njiraini* comes in because he is the expert…the issue of computers is by and large Njiraini's* docket…anything to do with computers Njiraini* has to be involved…if something went wrong and he does not sort it, then we reprimand him, reported ULR4 commenting on the ICTT in the library.

4.10.4 Disaster Recovery Teams

The researcher sought to find out whether there existed disaster recovery teams and what role(s) the members of the team played if such a team existed. In all the institutions studied, there were no data recovery centres established and no data recovery teams existed. However, one ICTD reported being in the final stages of developing a data recovery centre. The ICTD was also quick to mention that the institution did not have a data recovery plan to guide the establishment of data recovery teams. The disaster recovery plan was in its development stages in this institution. The ICTD hoped that the plan would guide the establishment of a data recovery team. The ICTD mentioned potential members of a future disaster recovery team as: the ICTD, the MIS manager, and the ICT infrastructure manager. Wong et al., (1994) as quoted by Chow and Ha (2009), note that DRP committee should consist of representatives from each functional unit so that their critical DRP events can be accurately gathered. The researcher noted with concern the omission of key personnel who should be in this team such as the finance officer, the PR officer, the institutional security manager, and the HR manager. According to the researcher, these personnel play key roles in recovery from a disaster.

4.10.5 Personnel Involved in Development of ICT Policies, Plans, and Programmes

Since majority of the target organizations had not developed ICT policies and programmes, the researcher looked at the personnel involved in the

development of ICT policies in one university that had established ICT related policies. The ICTDR2 mentioned that the ICT directorate had developed the ICT policies and approval was made through deans committee, senate, and launched from the office of the Vice Chancellor. This showed the seriousness with which this institution had taken in regard to their ICT infrastructure. Thus, the top management played a big role in the realization of the development of the policies.

4.11 Policies, Programmes and Plans for Disaster Preparedness and Mitigation in CBIS

The researcher aimed at assessing the policies, programmes, and disaster management plans in order to assess whether or not they addressed issues of disaster preparedness and mitigation in relation to library CBIS. The aim was to establish whether or not the institutions studied were aware of the importance of addressing the ICT disaster preparedness, mitigation, and recovery as demonstrated by existence (or lack thereof) of policies, plans, guidelines pertaining to prevention and recovery from disaster that might affect their library CBIS. Given the importance of ICT infrastructure as a core driver of higher education institutions in this era of technology, the researcher found it necessary to check the availability of these documents in order to assess the management awareness and commitment in this endeavor. To achieve this, the researcher collected data through the interviews and document analysis. The researcher also assessed the availability of the policies, programmes, and plans relating specifically to the institution library in addition to those of the institution at large on related issues. The findings were categorized into the following sub-themes:

i. Availability of policies, programmes and plans.

ii. Availability of ICT policies, programmes and plans.

iii. Disaster management issues for CBIS outlined in the ICT policies, programmes and plans.

iv. Accessibility of the policies, programmes, and plans by the members of the institution and the public.

4.11.1 Availability of Policies, Programmes and Plans

The researcher assessed the availability of various documents in the institutions studied that the researcher believed should incorporate ICT related issues such as ICT infrastructure, training, and strategic direction of the physical and non-physical ICT infrastructure. In this era of digital technology, ICT component is given prominence in organization libraries. The researcher aimed to determine whether these documents addressed ICT issues and in particularly disaster management of CBIS. The purpose was to illustrate the management awareness and commitment to ensure the organization runs smoothly in the face of a disaster affecting CBIS. The researcher collected various documents for analysis from the institutions studied. These were as shown in Table 4.7:

Table 4.7: Documents collected in each institution

UNIVERSITY	Documents reported by respondents	Documents collected
R	R ICT Security Policy R strategic plan (2012-2015) R library ICT policy	R ICT Security Policy R strategic plan (2012-2015) R library ICT policy
S	Strategic plan (2009-2012) Information Security Policy e-waste Management policy ICT Automation Policy and Strategy Security policy or S Electronic Payments Staff code of ethics	Strategic plan (2009-20012) Information Security Policy e-waste Management policy ICT Automation Policy and Strategy Security policy or S Electronic Payments

T	T library strategic plan T Library ICT policy	T library strategic plan
U	U Library ICT policy U Information Security Operation Manual. U Resource Use Security Policy and Network Usage	Library ICT policy

Source: Document analysis

From Table 4.7 above, it is evident that two of the institutions studied had developed their strategic plans. This meant that they knew where they were, where they were heading and how they would get there, and had put it down. Also, one of the institutions studied had policies guiding its ICT establishment and development. This indicated that the institution considered ICT infrastructure as an important aspect. As Eden and Matthews (1997) observe, disaster is inevitable and they, therefore, advise that disaster control plans need to be drawn and revised regularly.

In one of the institutions, there was no single policy except the library strategic plan. In this particular institution, there seemed to be no orderly way of handling ICT-related issues and no one seemed to know what the other party was doing in terms of ICT establishment and development. ICT issues were decentralized to departmental levels and each department was left to take charge of its own ICT issues, including backing up data, staffing, and maintenance among others. The ICT infrastructure was, therefore, in a state of want. As previously discussed, this institution's library had its server in a store. It had mirrored its server in the UK but had no other backup within the institution. As reported during the interviews, the institution's departments seemed to compete with one another in a very unhealthy manner such that it

depended on who knew who in the top management echelons for his/her voice to be heard.

Some documents were reported to be there during the interview sessions but they could not be availed. It was, therefore, hard to tell whether for sure these documents were available.

4.11.2 Availability of ICT Policies and Other Related Programmes and Plans

As much as the documents were available as shown in table 4.6 above, the researcher was also interested in determining the availability of documents that particularly addressed the ICT issues. The researcher aimed to assess whether the documents available addressed ICT-related issues on disaster management or business continuity in relation to the way ICT was handled in the organization or in the library. The findings showed that there were various documents in these institutions related to ICT.

The researcher confirmed the availability of these documents by accessing them from either the institutional website, borrowed them from the library through the library personnel or was given by the interviewees. This is as listed in Table 4.8 below:

Table 4.8: ICT-related documents available and analyzed

UNIVERSITY	DOCUMENTS COLLECTED	REMARKS
R	R ICT Security Policy R Library ICT Policy R Strategic Plan (2012-2015)	Produced in-house and not approved. Strategic Plan approved by top management

S	S Information Security Policy S e-waste Management Ppolicy S ICT Automation Policy and Strategy S Security Policy or S Electronic Payments S Strategic Plan (2009-2012)	All approved by the university top management
T	T Library Policy T Library Strategic Plan	..
U	U Library ICT Policy .	Produced in house and not approved

Source: Document analysis

Although the interviewees reported the availability of these documents, it was noted that some were not policies as such. They were actually rules and regulations which stipulated the dos and don'ts in the organization or the library and had not been approved by the management. Others were guidelines that outlined the dos and don'ts, the role of each person in the library and the penalties for not adhering to the rules and regulations of the library.

All the target institutions, there were no documented independent and structured user training programmes relating to ICT. Only one institution had embedded its training programme in one of its ICT policies. These documents were analysed as per issues related to disaster management.

4.11.3 Disaster Management Issues in CBIS

The documents collected were analyzed to ascertain the key issues addressing disaster mitigation, disaster preparedness, risk assessment, business continuity or disaster recovery. These are the key terms normally used to refer to disaster management as a broader term. The findings were summarized as per the institution and the documents in Table 4.6 (Page 56). These were as follows:

R University

This institution dedicated a whole chapter on ICT infrastructure in its strategic plan. ICT was indicated as a major pillar in its strategic goals and vision. Challenges facing ICT had been outlined in the strategic plan and the University had put it as a strategic goal to continue strengthening ICT facilities of the university. Among other things, flagship projects in the priority list were automation of university operations, installation of fiber optic, Voice over Internet Protocol (VoIP), and increased internet connectivity bandwidth, enhanced ICT maintenance and software development unit, establishment of smart card system for staff and students.

Some strategies to achieve the objectives among others included: establishment and strengthening of the ICT Directorate, expanding the existing intranet and internet connectivity, installation and enhancement of existing bandwidth, increasing number of staff trained on the use of ICT, formulation of an ICT policy, and enhancement of the university ICT infrastructure.

This showed that the university was well aware of the strategic vision regarding the ICT infrastructure. Though not directly mentioned, issues related to disaster management were incorporated into the strategic vision plan of the university.

S University

This institution had a wealth of policies guiding ICT development, management, and security. They had been launched by the top university management. They included the following:

Information security policy: This policy discussed in detail the following:

- the principles of information security; integrity, confidentiality, availability and accountability;

- Responsibility of information security; information owners, information custodians, information users, user managers and ICT security staff.
- Classification of information; public information, restricted information and internal use information.
- Access to information.
- Control of information security; among other issues.

Other issues outlined included standard practices regarding access to, use of, and rights related to use of their information system. This policy included measures to be taken to ensure the automation systems were secure. It also discussed in detail who was to do what, and when. Types of threats that would compromise security of CBIS were outlined and how these threats would be dealt with.

ICT Automation policy and strategy: This policy detailed strategic commitment of ICT infrastructure. It dedicated a whole section on information security, risk management, disaster recovery, and business continuity. This section outlined policies to guide data recovery procedures, standards to be followed, responsibilities of the key personnel, and the implementation strategy. In part the section read:

> … the University is committed to ensuring that the information it manages is appropriately secured to protect against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information, the existing ICT facilities, servers and network infrastructure in particular, have been designed and procured to provide the greatest possible resilience and reliability, the University shall produce an overall business continuity plan that shall inform ICT disaster management planners.

This showed the strong commitment the University had towards ensuring security of the ICT infrastructure. In its log frame of the implementation strategy, the information security management system (risk management, disaster recovery and business continuity) the following, among others, had been listed as strategic items/projects;

- Off-site data centres.
- Backup bandwidth.
- Antivirus.
- Staff capacity development in information audit which includes risk assessment, mitigation and/or treatment.
- Business continuity management which includes disaster management.
- Recovery and continuity of critical ICT services and functions.

The revision status annex of this policy also showed that the policy was regularly revised at least twice a year and the revisions were again launched by the top university management. This document also affirmed the institutional commitment to ensuring security of its ICT systems.

Security policy of S Electronic payments: This policy was a replica of the Information Security Policy. The departure was only in that it discussed issues related to electronic payment in the University.

e-**Waste Management Policy:** This policy discussed in detail how to handle the e-waste from the university ICT systems. This is a very critical aspect of disaster management as disposal methods used may jeopardize the security of the ICT functions, operations and services if not handled properly. Therefore, the researcher found it a very important document for the disposal of both physical and non-physical ICT systems. It is one aspect that is mostly ignored

by many institutions. This actually became an eye opener to the researcher as this is one policy document that the researcher did not even come across during literature review.

Strategic Plan: In the strategic plan of this university, ICT was discussed as a sub-section under resource requirements which was again a sub-section of situation analysis. This meant that ICT had not been recognized as a major strategic issue in this university. There was no mention of disaster management of ICT infrastructure. Although the institution had many documents discussing ICT related issues, it failed to recognize ICT systems as a major aspect in its strategic goals..Though strategic direction of ICT is outlined in the ICT automation policy and strategy, this was one aspect the researcher thought should have also been incorporated within the institutional strategic plan. This was a major omission and therefore, in terms of evaluation of the milestones achieved in relation to ICT related issues as ought to be outlined in the policy documents, there was nothing to guide on this.

U University

Library ICT Policy: Although the library had come up with an ICT policy which aimed at creating rules that aimed to limit, guide and manage the risk associated with unlimited use of ICT facilities, it fell short of what a policy document should include. It only had rules and regulations which governed use of ICT facilities and access to e-resources in the library. It was also in its initial stages of development and this was done in-house by the department. In terms of disaster management issues, the policy outlined a number of duties and responsibilities the ICT section should undertake to ensure security for CBIS. Some measures that ought to be taken to ensure that ICT facilities are protected had been outlined such as:

- Scanning of incoming messages, file downloads and storage devices for malicious codes such as viruses or Trojan horse.
- Sustaining user awareness of ICT policies and other policies.
- Offering training to users in the proper usage of ICT facilities.
- Technical issues relating to monitoring of ICT network and other ICT resources.

This policy also outlined what each section of the library should do to ensure security of ICT system as follows:

- Undertake to ensure ICT facilities are taken care of.
- Provide proper physical environment for equipment.
- Provide individuals with resources for required backups and virus protection.

Measures such as use of passwords were scantly outlined. It was noted, therefore, that this policy was more or less a working manual regarding the ICT-related activities rather than an ICT Policy.

4.11.4 Accessibility of Policies, Programmes and Plans

The researcher was interested in assessing the methods or channels used to avail the documents to the employees or the public as well as the students. This was meant to determine if the documents were confidential documents, and if the public, employees and the students in that case knew what was expected of them. It was also termed as a method of training, creating awareness, assessment and evaluation. The findings were as follows:

Three of the institutions studied did not avail their documents through the university website. Only S university availed all its documents as listed in Table 4.6 (Page 56) through the University website. The strategic plan was also available in the library open shelves for anyone authorized to read or

borrow from the library to do so. Therefore, the public was free to peruse what S university had in terms of their ICT policies and the strategic direction of the university. In this institution, the top management was actively involved in the development of the ICT policies and it was, therefore, easy for them to support what was outlined in the policy. It was also noted that these documents had been launched by the top university management unlike in the other institutions where top management were not involved.

Two of the other institutions provided only the library ICT policy and guidelines through the library website. This included the R university library and T university library. Most of the documents listed in Table 4.6 (Page 56) above were in the custody of the heads of particular departments. This indicated that the documents were neither for circulation nor for public consumption. In fact, most of them were drafts and had not been finalized. It was also reported that they were drawn by the members of those particular departments only. They were treated as confidential documents and even some members of these departments were not sure of their existence. In this case, the researcher could not access some of them though they had been reported to be available during the interview.

4.12 Challenges Faced by Libraries in Preparing for and Mitigating against Disaster for CBIS

The researcher envisaged that ICT was a field that was tremendously growing, coupled with various challenges. The researcher therefore aimed at finding out those that were faced in the endeavour to prepare and mitigate disaster for CBIS in the library. The following challenges were reported by various respondents:

i. Procurement of ICT related infrastructure

In all the target institutions, it was reported that the procurement process took long even for items that were needed urgently. In some cases the required items were never even provided for at all, or they were delayed:

> we got the approval late and we were given a small budget, what we did, we did part of the data centre but not the full disaster recovery centre…other critical bits of the data recovery centre are still outstanding, commented ICTDR1.

In another instance ISLR1 talked of purchase of padlocks that had been requisitioned for but had not been supplied a year later, leaving the library with no options but to look for alternative means of preventing computer vandalism. "The padlocks were requisitioned for in September 2011, up today (2012) we are still waiting for these padlocks to be supplied," ISLR1 noted.

Bureaucracy in the institutions was also seen as a hindrance to smooth running of the ICT section in the library. To install a system it had to be tendered, then the tender had to be approved, and this process would take a month, two or three. One ugly situation was reported to have happened where requisition documents were reported to have been misplaced within the finance department on several occasions. For instance one, UL had this to say;

> …we have had an ugly period where you send the requisition to buy things (computing equipment) and they (finance office) keep hiding books, lamented ULR4.

ii. Dependency on the ICT Directorate and Other Departments

In most cases, libraries depended on other departments such as ICT department to give direction or to facilitate ordering, purchase of ICT facilities, maintenance, backup and hosting of library main servers. This brought about delays and sometimes the staff in the library seemed not to

know what the ICT directorate had done especially in terms of backing up of library databases. In one of the institutions, it was reported that the library servers could go down over the weekends and the ISL had no access to them since they were in the custody of the ICT directorate. This denied users access to essential services and resources as reported by one ISL:

> The biggest challenge we have is the location of the server…where the server is located, it is not accessible to library ICT staff. Even if I was told it was not working I would not walk into the institution and switch it on, commented ISLR1.

Finance department, on the other hand, controlled the budget and the procurement process while human resource management was in-charge of hiring of personnel. In another library, it was reported that the finance officer delegated matters related to library ICT to the ICT directorate which delayed the acquisition of computing equipment in the library. In relation to this, one UL lamented:

> …without any discussion, the finance officer decided on matters related to computers be handled by (ICT Director) We are now to tell [the ICT director] what we want and buys. This brings about delays and since then (two years by 2012) we have not yet received anything yet, commented ULR4.

> How long the generators can take depends on availability of fuel, we have to order fuel on constant supply which means that the ICT [department] has to work hand in hand with estates [department], have to work hand in hand with procurement [department] and finance [department]to ensure all these elements are there when needed. It is usually not an easy task, commented ICTDR1.

iii. Unscrupulous computer students.

Activities of students taking computer science courses were reported as a main challenge to the security of CBIS. Students wanted to experiment with what they had learnt in class and it was noted that this group of students were ahead

of ICT personnel in the library skills and knowledge related to ICT. All the libraries reported that students hacked the systems, vandalized the computers, installed programmes into the library computers and other times stole parts of the computers like the mice. The challenge was for the ICT personnel in the library to keep upgrading their skills to remain relevant and also to be vigilant on what the students may do to the CBIS because it was not predictable. Curbing students' actions became a challenge to the library staff as students devised several ways of bypassing measures put in place. Commenting on hacking, one ICTD had this to say:

> We have open systems to students and staff twenty four hours seven days a week you have to be on the lookout for attacks that may come from whatever when our systems are open to the public ream, reported ICTDR4.

iv. Inadequacy of trained staff

Adequate and well-trained staff plays a major role in any organization. Lack of training therefore, hampers its smooth running. Any organization should endeavour to employ and retain adequate and well trained employees. In a number of the target universities, this seemed not to be the case. Inadequate number of trained ICT staff was hindered by the staff recruitment procedures, qualified staff turnover as well as remuneration of qualified staff. One university librarian mentioned that the process of writing the library ICT policy was hindered by high staff turnover where:

> we had begun writing them[policies],and the problem was we reached a level, and all the staff who were there left. The last four years we lost very senior people, the sad bit is that they do the work and the University frustrates them by not remunerating then accordingly and they leave, commented ULR4.

This was in relation to writing of the library ICT policy and lack of proper remuneration of staff. This was echoed by ICTDR4:

> personnel is another challenge we face in our area. I think since I came here I have had many groups of people to work with, about five groups…every time I get new people I have to take them through training and when they are good they are on their next plane. I think salaries are a contributing factor and lack of clear path of professional growth.

In another university, the ICTDR1 had the same sentiments:

> Sometimes we do not get adequate well qualified staff. We need somebody with high qualifications but when we advertise we do not get right people to apply for the job and we end up hiring people who are not well qualified for the job, comments ICTDR1.

ISLR1 reported lack of adequate number of staff in the ICT section and observed: "there are many things to attend to and we have few personnel…I am the only person working in ICT section, others are employed on casual basis."

v. **Dealing with employee work culture, awareness and resistance to change**

Lack of seriousness, staff culture, and negative attitude impacted negatively on the way ICT related issues were handled. The findings revealed that resistance to change was a hindrance to the automation process of some libraries. Although it was reported the management was responsive to the needs of ICT related issues, report from one public university indicated that employees lacked ownership which in essence affected the operations of the ICT department. In relation to this ICTDR2 noted:

> apart from resources and getting responsive management, there is issue of work culture essentially being a public university, it seems we have borrowed a lot from public service where 'hii ni kazi ya university' (this is university's work)

> there is some sense of lack of urgency whenever anything happens and that is a key monster to tackle,

ICCTR1 also observed:

> Staffs do not want to change from normal ways of doing things. Another challenge is resistant user group, you tell a user doesn't do this and that, and they repeat it tomorrow.

Lack of awareness on security to CBIS by employees was shown by the way usernames and passwords were handled by employees. In a number of cases, employees were reported to share passwords while others gave password to relatives where sensitive data were accessed by users who were not authorized to access. This resulted to hacking of the CBIS. ICTDR1 observed:

> Lack of awareness is not by management only it is by everybody. Sometimes lecturers give passwords to their children and their people in the department and threats have been there and most of them are internal like changing of marks where lecturers knowingly or unknowingly give out passwords while others hack the system.

vi. Lack of guidelines on ICT security issues

Three of the target libraries had both positions of ISL and ICTT which brought about conflict as noted by the researcher. The ISL was senior to ICTT, which meant that he/she was to work under the ISL. In terms of skills, experience and training on ICT issues, the ICTT had better education and skills compared to ISL. This meant that the ISL could not give lead to ICT related issues but he/she was a learner under his/her junior. This did not auger well between these two staff in most cases. This in effect affected the smooth operations of the ICT section of the library and in one library, it was so bad and one could feel the rivalry between them from the way the interviewees answered the questions. There seemed to be a blame game from the ISL and the ICTT.

Guidelines on who handled what or who was in charge of what in terms of library CBIS was not well-outlined.

vii. Low levels of training

Except in one institution where training was structured and the library staff were continuously trained, other libraries did not have well-structured training and especially training on security issues. Many respondents reported lack of training on ICT security-related issues. Implementing ICT security-related measures by people who are not well verse with ICT was seen as a big challenge.

viii. Lack of enough funding

Lack of enough funding or delays in providing funds to buy necessary computing equipment was cited as a challenge. In some cases this hindered the establishment of disaster recovery centres, which is a key component in disaster preparedness and mitigation for CBIS. ULR4 lamented that:

> The library has a budget that covers [ICT infrastructure] but one of the things we've found out in the University is that we reach a level where they[finance] simply don't buy what we want they [Finance department] have kept quiet without providing us with money to buy more computers but we are still fighting

This showed that financing ICT infrastructure was a challenge. Without appropriate and adequate ICT infrastructure, there was tendency to deny users access to essential services and resources and at the same time hampering effective and efficient running of the library. ICT computing equipment was viewed as an expensive venture and money was never enough to provide for the much needed ICT infrastructure. Again, ICT directorate was a service department and a direct benefit to the institution was not easy to quantify. Therefore, justifying funds through budget allocation was a big challenge. At

times, findings showed that during budgeting, it was not possible to itemize those for the ICT which at times resulted to under-budgeting.

One ICTD elaborated this challenge by saying the following;

> The ICT environment especially in public institutions compete for traditional budget of the institution so there is a scenario you want to have the very best but also it is seen as an extra unwarranted expenditure on the institution therefore when you talk of the capacity or potential to establish a data recovery centre and continuity management system, it is not an area where people have invested because there is a dilemma …you have to really get enough money to invest in data recovery centre that cost equivalent to fifty thousand computers so there is competition between the real need and …there is real battle for investment for what the customers need, and investing in what would ensure that the customers interests are also protected. So, not many of our institutions have invested in data recovery systems the way they should be actually done for that reason we are talking of small measures here and there, commented ICTDR1.

ix. Low levels of awareness among top management of the organization

The top management of any organization plays a major role in the running of the organization. They influence, among other things, staffing, policy development and financing. The awareness level of the management in terms of disaster recovery issues also influences the direction which the disaster preparedness and mitigation for CBIS take. Straub (1998) observes:

> Information security continues to be ignored by top managers, middle managers, and employees alike. Many managers are not well versed on the nature of system risks likely leading to inadequate protected systems.

The study concurs with this where low level of awareness on ICT related issues among top managers was cited. In one instance, top management of one institution was reported to have taken keen interest on disaster management of CBIS when the IT system was compromised. Creating awareness among top managers and middle managers was hampered by change in position and

especially where structured training was not carried out. Commenting on this ICTDR1 has this to say:

> awareness is a challenge because sometimes the management may not be aware of what you[ICT directorate] are talking about. They got good awareness when we got a threat where somebody was able to hack in the database. At the same time deans have changed, most of the chairmen of the departments have changed and it has became a challenge in creating awareness on the management of passwords at the departmental level.

Kundu (2004) observes that there is need to understand the real nature of disaster if mangers are going to be able to carry out adequate contingency planning.

x. Lack of policy and guidelines

Three of the target institutions did not have written policies on ICT related issues. Yet, policies act as reference point or guide on what ought to be done. Foltz (2005) notes that written policy statements explaining the correct and incorrect use of organizational information systems are thought to reduce the amount of misuse within an organization and are considered to be a cornerstone of security.

xi. Employment procedures and terms of service

This was seen as a challenge as adequately and qualified staff to deal with ICT related issues lacked in the institutions. Hiring and retaining qualified ICT personnel was seen as a challenge. To explain this, ICTDR1 lamented:

> We had some advert where we needed 6 positions and we put a criterion for a Master's degree. The grade is tied to an academic qualification where minimum is a master's degree in ICT related field. People in the industry who are qualified to do same kind of work do not have a Master's degree but have first degree. We could not therefore get people to apply for the positions.

In the same institution, the ICTDR1 reported to have been hired without a job description and therefore had to draw a job description for this position. This should have been handled the other way round. The management, therefore, had no one to pin down if there was failure in the institution's CBIS as the ICTD did not have an official job description. Such an ICT director in the researcher's opinion will draw a job description that favours him/her or one that outlines only areas he/she is comfortable dealing with.

In another instances, the ICTTR1 had been hired on contract basis. This meant that there was still much that the staff could not handle and especially security related matters sincere some of the information handled by ICT personnel could not be accessed by staff who were not employed on permanent basis as it was seen as a security risk.

xii. Increasing user population

In one of the target institutions, the increase in user population was seen as a major challenge. This was because the level of vandalism increased and the traffic to the computer labs increased. Again, many users seemed to have been denied access to computing facilities for essential services and resources offered by the library, as reported by ISLs and ICCTs. In this regard, internet connectivity became slow and libraries lacked enough facilities to cater for the increased population. The increased numbers also hindered proper surveillance within the library.

xiii. Size and nature of library building

The findings revealed that some respondents felt the library buildings were so big to provide adequate surveillance in areas where computers were located. Others felt that the ICT infrastructure was not taken into consideration during the planning stage of the building construction. In this case, proper ICT

infrastructures were not in their rightful place. In terms of ICT infrastructure development*:*

> the traditional institutions constructed building and nobody consulted ICT personnel to say what the ICT requirements of that building were. Therefore the buildings took one or two years without anything to do with ICT infrastructure because it was not a key consideration at the planning stage, observed ICTDR4.

On the same issue, CLR1 also commented about the size of the library building and had this to say:

> the place is very big we cannot afford to have everywhere we have computers manned except in the lab. The size of the building is so big and it is not possible for guards to go round at any one given time, the windows and doors have no grills to deter a thief.

xiv. Changes in technology

Technology changes at a very fast pace. This means that staffs have to upgrade their education and skills to match the changes. To keep intadem with these changes means investing on these changes both on physical facilities and in skills. This was reported as a challenge since the institutions were not able to keep abreast with this and were therefore:

> not prepared because the field of information security is dynamic, we never know which new routines can come up. In one instance an equipment was tendered but by the time we were through with technical evaluations and the award of tender, the equipment that was quoted was no longer in supply, so we had to go through a lengthy process of change. The dilemma was, do we recommend what we knew or do we recommend what is coming in future? In fact you would recommend the future one and after that another one comes with better functionalities so we really have a challenge there, observed ISLR3.

Commenting on the same, one ICCT also had this to say:

> the people who make anti-viruses are the same people who come up with the viruses, so we have to look for some other software to try and clean out some viruses.

> For now the ant virus has helped deal with viruses but as you know technology, they may come with a way to bypass that, notes ICCTR1.

Due to the students taking software engineering and computer science, the staff ought to be ahead of the students and anticipate what they what they are likely to do and put the necessary measures. This again becomes a challenge as students keep learning new things every day and trying ways of bypassing measures that have been put in place.

CHAPTER FIVE

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This Chapter presents the summary, conclusions, and recommendations of the study. It is guided by the theme of the study which was to investigate the disaster preparedness and mitigation for CBIS in selected university libraries in Kenya. The summary of the key findings is presented, conclusions made, and recommendations are given. The study, also, presents identified knowledge gaps and further research.

5.2 Summary of the Findings

This is guided by the research objectives and research questions. These were grouped according to themes that were identified in Chapter Four. The themes included the following:

i. Automation in libraries, electronic information resources and services.
ii. Awareness and perception of CBIS.
iii. Awareness and perception of security for CBIS.
iv. Threats experienced in libraries related to CBIS.
v. Measures used to prevent and mitigate disaster for CBIS.
vi. Indicators of unpreparedness for disaster related to CBIS.
vii. Personnel involved in disaster preparedness and mitigation for CBIS.
viii. Policies, programmes and plans on disaster preparedness and mitigation for CBIS.
ix. Challenges associated with disaster management for CBIS.

5.2.1 Automation in libraries, electronic information resources and services

The findings showed that the target libraries had incorporated electronic resources in their libraries. These were in-house developed and others were through subscriptions. The e-services were also identified. The e-resources included e-journals, e-books, institutional digitized collection referred to us Institutional Repositories (IR), digitized examination past papers among others. Use of LMS such as Koha, Sir Mandarin was identified as well as internet services, computers for research purposes, OPAC, and library websites. This meant that libraries had not been left behind in the era of information age. They had embraced technology to ensure efficient service delivery as well as offer diverse and wide range of information resources even to their remote users.

5.2.2 Awareness and Perception of CBIS

The findings revealed that the respondents had varied views of what CBIS was. Those who dealt directly with CBIS had a good perception and understanding. These included the ICTDs and ICTTs. Though the ISL was directly involved, the understanding of CBIS could not match that of ICTDs and ICTTs.

Also, the ICTDs and ICTTs had training in ICT related field. The ISLs and CLs had no training on ICT-related field. Therefore, education and training play a major role in the awareness, understanding and perception of CBIS.

5.2.3 Awareness, Understanding and Perception of Security for CBIS

The respondents had varied levels of awareness and perception for security of CBIS. Better awareness and understanding were evident among the ICTDs and ICTTs. This was shown by the level of detail in which they explained the

measures that were and should be used to secure CBIS. Although a number of measures discussed by this group had not been taken in the respective libraries, they hoped to do so in future. This included such measures as establishment of data recovery centre (DRC), DR planning and cloud computing.

The ISLs also showed understanding of what security entailed. The level of awareness and detail again varied from that of ICTDs and ICTTs. This seemed to be lower than that of ICTDs and ICTTs. All CLs and ULs shallowly discussed this issue. In fact, all talked about security guards, firefighting equipment, and M3 security system at exit door.

It can be concluded that the education and training played a major role in the understanding and awareness of security of CBIS. This was because three of the ICTDs had a good grasp of security of CBIS. They had been trained, that is, had Master's degree in ICT-related fields. They mentioned having taken courses or training in security in CBIS. The ICTTs also indicated that they had training on issues related to security of ICT, though not a full course had been taken. This group had bachelor's degree in ICT related courses.

The ULs, ISLs and CLs had training in library and information science related fields. The knowledge gained on ICT was through working with e-resources in their respective libraries. Their understanding of security of CBIS was limited to the very basic issues of backups, passwords and guards.

5.2.4 Threats to CBIS

The study revealed that libraries experienced a number of threats and disasters related to the CBIS in the libraries. These included:

Theft and vandalism: Computing equipment such as keyboards, mice, electric cables, network cables, video recorder were on several occasions stolen or vandalized. Computers were reported to have been found without hard disks or CD/DVD drives.

Change of settings, software downloads and hacking of systems: Users were reported to have changed software settings thus tampering with the way the software functioned. Unauthorised software were also downloaded to the library computers making the system malfunction, overloaded and, at other times, allowing unauthorized functions/activities to be carried out. Unauthorised access through hacking threatened the operations of the CBIS in the library.

Employees work culture, negative attitude and lack of training on IT skills: Employees were seen to have negative attitude and especially in public universities. They lacked sense of ownership and lacked training on IT skills as reported by the respondents belonging to ULs, ISLs and ICTTs groups. Lack of IT training and negative attitude meant that the CBIS were not well-protected and actions that could cause disaster were reported such as sharing of passwords.

Fast change of technology: As the technology changed so did the skills to operate it. Upgrading of the system was also required to accommodate the changing technological environment. This was seen as a threat since at times data was lost in a bid to upgrade to newer systems. Required skills were also not sometimes available to function with newer technologies.

Viruses: Virus**es** were introduced to the CBIS on a daily basis. They were seen as a threat since no one knew what virus may be introduced next. In some

instances, it was reported that the anti-viruses were normally out of date and therefore, viruses were seen as a threat. Loss of data was reported due to virus attacks.

Power failure and power surges: Majority saw this as a threat to data and service delivery. Available generators were not able to provide power for a long time except in one library where this was not seen as a problem.

Dust: In a few cases, this was seen as a threat to CBIS in the library since computing equipment such as servers were affected by dust. It was noted in one library that the server had been put on the floor which was dusty and the room was rarely cleaned.

Building (size and nature): In one library, one respondent mentioned the size of the library building as a major threat to CBIS since the building was so big that it was not possible to man all the areas where computers were located. This caused vandalism to computers.

Water: In two of the libraries studied, water leakage and flooding were reported to have caused damage to the CBIS. This was where computers had been housed at the top floor and the basement of the library buildings.

Lack of connectivity: Unplugged network and electrical cables were reported to have caused data loss in the library. This also caused denial of service to library clients.

This meant that CBIS were vulnerable to a myriad of threats which could cause disasters. Any of the above threats could disrupt the operations of the library. Therefore, it was necessary to take precautions to mitigate disaster or

even prepare due to the fact that any of these threats could happen in varying degrees at any one time.

5.2.5 Preparedness for Disaster

The study sought to find out what the respondents thought about the level of preparedness for disaster. The findings revealed that the respondents were not certain whether or not they were well-prepared for a disaster. One respondent indicated that they were prepared to a small scale according to their budgetary allocations. Also, another reported that preparedness had been taken according to threats that had been experienced. The ICTDs, ICTTs and ISLs indicated that it was not possible to fully prepare and mitigate against disaster. This concurred with Dhillo (2001), who observed that no system could be made absolutely secure. Thus, findings concluded that ICT field is dynamic and it is not possible to know when a disaster would strike. This is because of the earlier mentioned myriad of problems.

5.2.6. Measures and Controls Taken

The target libraries and institutions had prepared and mitigated against disaster that could affect CBIS. The findings revealed that all the target libraries had taken several measures to ensure their CBIS were protected or there would be business tomorrow even if a disaster happened. These measures were grouped into three categories: physical, procedural and technical measures.

5.2.6.1 Physical Measures

These included:

i. Tying cables and peripherals together using steel wire or tie backs to curb vandalism. The libraries studied experienced the problem of vandalism of their computing equipment. To curb or reduce this, steel wire and tie backs had been used to tie peripherals and cables together as shown in Plate 4.2 (Page 51) Steel wire had also been used by one library to prevent opening of the CPU cabinet as shown in Plate 4.1 (Page 51)

ii. Use of padlocks to lock up CPUs cabinet. Some computer models such as Dell were reported to be very easy target for opening the CPU cabinet. To curb this, padlocks had been used in one of the libraries as shown in Plate 4.6 (Page 56.)

iii. Engraving the equipment with a unique code: two of the libraries studied had engraved unique identification to the computer devices with an aim of preventing theft of computer equipment as shown in Plate 4.7 (page 108)

iv. Use of personnel (both library staff and the security guards): In all the libraries studied, security guards had been employed to man the library as a whole. The guards were meant to deter would-be vandals and at the same time check users as they exited the library to deter theft of computing equipment. The library staff were responsible for ensuring security of CBIS by being vigilant at all times.

v. Magnetizing equipment using magnetic strips. In one of the libraries, magnetic strips that were detected by the M3 security gate at the exit door had been put at strategic places of the computing equipment. This was reported to have reduced theft of equipment and even facilitated identification of those who attempted to steal from the library.

vi. Use of CCTVs: One of the libraries had installed CCTVS at strategic places where computers were located such as OPAC area. This facilitated

identification of those who vandalized computers or did illegal activities to the CBIS.

This showed that vandalism was a major threat to CBIS and libraries had taken the necessary steps or measures to curb or reduce this problem. Although the study did not investigate the causes of vandalism and theft, one respondent talked of culture, economic hardships and availability of market for the equipment.

5.2.6.2 Procedural Measures

Apart from physical measures, procedural measures taken were also identified. These included:

i. Clocking or recording usage of e-resources or computing equipment: In all the libraries studied, the users were required to record their details and show their identification cards. This was to ensure only authorized persons used the computing equipment. The other reason was to allow the library staffs give an account of who used what in case of a problem.

ii. Training and sensitization: Users of CBIS were sensitized through workshops and seminars. Some of the issues covered related to the use of passwords, authorisation and handling of new systems.

iii. Use of anti-virus: The anti-virus was used to curb the problems of viruses. Different anti-viruses were used and the upgrading of the anti-viruses varied from one institution to another.

iv. Use of firewalls: Firewall was a measure used to protect the network from external threats. Threats such as hacking of the system were seen as a major threat where the firewall was used to curb this.

v. Policies: In one institution where policies had been developed and approved by the university management, these were seen as a measure

employed to protect the CBIS. The policies outlined what should be done, by who and when. Through the sensitization process of what the policies had, members of staff were made aware about the threats and measures that needed to be taken.

vi. Mirroring/ redundancy: All the libraries studied reported that servers were used to create a mirror copy of the databases.

5.2.6.3 Technical Measures

Technical measures identified included the following:

i. Usernames and passwords: All the libraries studied reported use of usernames and passwords as the most basic measure to ensure security of CBIS. Management, creation and use of passwords differed from one library to another with some sharing passwords.

ii. Backup (data backup, power backup and connectivity backup): Mirroring and duplication of data were done to ensure that if anything happened to the original data, backup would be used for resumption of services. Due to erratic nature of power supply, power backup through generators was provided. In addition to this, internet connectivity was provided through different internet providers to ensure continued internet services.

iii. Use of rights and privileges: The libraries studied were automated. Through the library management system (LMS), different levels of access had been provided for different categories of users as a way of ensuring security or preventing tampering with the operations of the library.

iv. Authorization and access control: This was done to the computer labs and server rooms to ensure only authorized persons used the computers or accessed sensitive data from the server. Authorization and access control were done through clocking and discouraging staff from using computers in their colleagues' offices.

v. Magnetizing: Use of magnetic strips that were detected by the M3 security gate was used by one library to discourage theft of computing equipment.

Other measures included:

i. Provision of adequate budget which was reported by one university as a way of ensuring that computing equipment could be bought quickly incase of theft or damage
ii. Insurance: Insurance cover for any loss of computers had been taken by one of the libraries.
iii. Encryption: One institution mentioned use of encryption software to tag computers such that if theft occurred, then it was possible to track them.
iv. Warranty: All the libraries reported warranty as a measure used to ensure computing equipment remained in good condition.
v. Software: Few libraries reported use of LINUX software for the server data backup to ensure virus attacks were eliminated. It was noted that virus attacks did not penetrate systems that were LINUX based.
vi. Disabling drives. In one library, drives were disabled to prevent unauthorized installation of software to the library system.

This showed that the institutions had taken necessary measures to ensure data, equipment and other facilities were well-protected against possible dangers. This also showed the personnel involved with ICT related issues were aware of the threats and the effects they could cause to service delivery and smooth operations of the organization.

5.2.7 Indicators of Unpreparedness

Though a number of measures had been taken to ensure the libraries were prepared and mitigated against disaster that could occur, the finding revealed

that there were a number of instances that contradicted this or showed lack of preparedness. These included:

i. Reckless lying of electrical cables and network cables: Majority of the libraries had the network and electrical cables lying on the flow recklessly. This in itself could cause denial of service due to either vandalism or unplugging of the cables from the sockets.

ii. Location of backup servers, server rooms and other networking devices: In all the libraries studied, backup servers were put in rooms that were not well-ventilated and some of them were so dusty. Rooms set aside as server rooms were located in the basement of the library buildings and some doubled as stores. In one of the libraries, networking devices such as the gateway was located in the basement which was prone to flooding and switches were placed along the corridors and this could encourage vandalism.

iii. Inadequate power backups and lack of electric filters: Majority of the libraries reported use of generators for power backup but also noted that the generators were not very reliable and sometimes did not last long. None of the libraries had installed electric filters to their computers.

iv. Lack of policies, training programmes and disaster management plans as well as lack of DR centres: Policies give guidelines on what to be done when and by whom. Majority of the libraries studied lacked disaster management policies and, therefore, activities geared towards preparedness and mitigation against disaster were handled through personal initiatives by personnel dealing with ICT.

v. Lack of cooperation between the library department and ICT directorate: Majority of the libraries studied reported lack of a well-coordinated way of handling ICT related issues between the library and the ICT directorate.

The above showed that the issue of preparedness and mitigation for CBIS had not been taken seriously. This could also mean that the libraries or the institutions at large had not suffered any major blow to give rise to the urgent need of and securing cables and developing disaster management policies.

5.2.8 Personnel Involved

Disaster management is in most cases determined by the personnel involved and given the responsibility to spearhead the activities as well as the awareness and knowledge level of the people concerned. The researcher, therefore, sought to assess the personnel involved or given the responsibility to spearhead the ICT-related issues in the organization. To achieve this, the researcher investigated a number of issues which included: top management support and role in disaster preparedness and mitigation for CBIS; training of staff; education, knowledge and skills of key personnel involved with CBIS; disaster recovery teams and personnel involved in development of ICT policies, plans and programmes.

5.2.8.1 Role of Management in Disaster Preparedness and Mitigation in CBIS

Majority of the respondents reported that the top management was very supportive in terms of budgetary allocation and they also listened to the ICTD for guidance and direction for the ICT directorate to take. They also mentioned that the top management got involved in policy development although very few institutions had drawn the policies and strategic plans related to ICT. The support depended on the advice given to them by the ICT directorate.

This would only mean that the top management had not championed the direction in which ICT took. Majority took a back seat and left this to the

ICTD who in essence had to keep “fighting” for budget allocation of ICT related development.

The ICT infrastructure is expensive and justification of such expenses in the budget allocation may not have been understood by some of the management. Therefore, establishment of DR centre had not been realized as the top management was not fully aware of the impact that lack of this would have to the organization.

5.2.8.2 Training

Training is a critical aspect in ensuring that people are aware of what disaster management entails. It also ensures that people become conscious and take the necessary measures to ensure the CBIS are well-protected and the impact that this could have if they were not protected. Majority of the institutions had not taken training as an important aspect. It was, therefore, not carried out and there was no structured way or methods that had been drawn to take care of the training. Only one institution carried out structured training to sensitize staff on matters of ICT security.

In conclusion, training had not been taken seriously as a measure to curb insecurity of CBIS. This, therefore, left many people unaware of what ICT security entailed and what role each person played to ensure that the ICT systems were secure.

5.2.8.3 Education Training and Skills of Personnel Involved in CBIS

To do the right thing, education, training and skills played a major role in ensuring that the right things were done.

The findings revealed the following:

i. Though the UL and DUL had education up to Master's level and above in some cases, the training was not related to ICT. This group of respondents was, therefore, not conversant with ICT related issues.

ii. The ICTD and ICTT had education and training in ICT-related issues including the security measures that ought to be taken.

iii. The ISL had training in the field of librarianship but not in ICT-related issues but needed a lot of guidance and especially the technical aspect of ICT. It was also evident that they did not take the lead on matters related to ICT in the libraries. Rather, the ICTT gave direction though this person was junior to the ISL.

This did not, therefore, ensure proper coordination between the different groups involved. In the library for example, it was evident that the ICTT looked upon the ISL to give guidance being the person he was working under. The ISL, for example was not able to guide the ICTT on ICT-related issues because he did not have better understanding and knowledge related to ICT.

5.2.8.4 Disaster Recovery Teams

The DR teams were non-existent in all the institutions. This was from the fact that DR centres had not been established. Also, the DR planning had not been put in place. Only one institution was in its final stages of establishment of DR centre and the DRP was not in place which would guide in the establishment of DR team. The lack of disaster team meant that if a disaster occurred, the institution would take a long time to recover. This was because the line of action to be taken by persons who could be involved and their responsibilities had not been outlined. It would, therefore, be total confusion in the organization

5.2.9 Policies, Programmes and Plans Related to Disaster Management for CBIS

The research sought to assess the policies or programmes and plans related to CBIS. The findings were grouped according to the following sub-themes:

5.2.9.1 Availability of Policies, Programmes and Plans

The findings revealed that several documents were available touching on issues related to ICT. Among the documents were the following:

i. Strategic plans.
i. ICT policies.
ii. Information security policies.

It was evident that majority of the libraries and universities had developed some policies, guidelines or rules on the smooth running of ICT related issues. However, the researcher noted that majority of documents labeled as ICT policies fell short of what a policy document entails. Many were working manuals and others were just rules and regulations on ICT use.

The researcher also noted that a good number of documents that had been reported to be available were not availed to the researcher. The researcher therefore concluded that either the respondents indicating the documents existed or probably they did not exist and were ashamed to say so since these are important documents in an organization. The other reason could have been that the documents are not well written or they were just draft documents which the respondent was not comfortable giving. Another reason could have been they are considered confidential and therefore the respondents were not willing to give them out.

5.2.9.2 Availability of ICT Policies, Programmes and Plans

The study aimed to assess the availability of documents related to ICT. The researcher therefore requested the interviewees to avail the documents they

reported they had in the institution or in the library. They were collected from the interviewees, borrowed from the library through the librarians or downloaded from the university websites. Through this, the researcher aimed to assess whether the documents were considered confidential documents or they were available to the public.

Majority of the documents availed to the researcher were not policies as such but rules governing the use, the dos and don'ts. They had also not been approved by the management and operated only within the library. One institution had developed a number of ICT related policies and had been obtained through the university website.

5.2.9.3 Issues Relating to Disaster Management for CBIS

The finding revealed that only one university had taken up writing of ICT policies seriously. It had, therefore, developed several policies related to ICT infrastructure. These included the following:

i. Information security policy.
ii. e-waste management policy.
iii. ICT automation policy and strategy.
iv. Security policy or S electronic payments.

These policies covered in detail issues related to disaster management for CBIS in S university such as: standard practices regarding access to, use of, and rights related to the use of information security, data recovery procedures, responsibility of key personnel, handling e-waste from the university ICT systems, among others. The top management had been involved and endorsed the development of these documents. This meant that they were official university documents. This showed the commitment that the institution had towards ensuring security of ICT infrastructure.

The rest of the institutions had come up with documents referred to as ICT policy. But these documents had not yet been endorsed by the top management of the organization and were, therefore, in their draft form. This meant that disaster management for CBIS took a back seat in these organizations.

5.2.9.4 Accessibility of the Policies and Plans

It is one thing to develop the policies and plans and it is another for the members of the organization to know what has been developed and what these documents cover. The study found that only in one organization the documents listed in Table 4.7 (Page 108) were accessible to the larger community of the organization and the entire public. The organization had posted all its documents to the university website from where any person was free to access, read or download.

Majority of the other organizations did not have their documents easily accessible by members of the organization. During the interviews, majority of the respondents referred the researcher to the person who had the custody of the documents. The others gave the researcher the documents and especially the UL and ICTD.

In some libraries, what was termed as library ICT policy had been posted to the library website. But on perusing the documents, these were not policies as such. Hence, most libraries seemed to lack ICT policies. Distribution of the said policies was not also guaranteed. Furthermore, the documents were not university official documents since they had not been launched by the university management and, therefore, belonged to the mother departments.

5.2.10 Challenges

The researcher sought to find out the challenges experienced in the endeavor to secure the CBIS. The study revealed that there were several challenges as listed below:

i. Procurement procedures of ICT related infrastructure: These took a long time to be completed. Hence, there were delays to provide required equipment or sometimes they were not delivered at all.

ii. Dependency of ICT Directorate and other departments: Majority of the libraries studied depended on other departments such as ICT Directorate, Finance Department and Human Resource Department. This dependency in most cases brought about delays, mismatch between the needs of the library and what could be provided for.

iii. Dealing with students' actions: Students were reported to hack the systems, install unauthorised software and, at other times, vandalise the systems. All the target libraries reported that dealing with student behaviour became a challenge and especially those who took computer science courses.

iv. Preventing hacking from system users: Users were reported to be always on the lookout for ways of hacking the CBIS. Sometimes it became difficult to control such actions.

v. Providing adequate qualified staff: All the libraries and ICT directorate reported that retention of qualified ICT staff was a challenge coupled with challenges of hiring adequate number of qualified ICT staff. There was high staff turnover and low remuneration of ICT personnel compared to what was paid to equivalent cadres of staff in the industries.

vi. Employee/staff: Members of staff were reported to lack positive attitude towards ICT-related issues. There was resistance to change and lack of awareness of what disaster management for CBIS entailed. It therefore, became a challenge to deal with employees who are not responsive to ICT needs of the library.

vii. Lack of policies and guidelines: Majority of the libraries and the institutions at large lacked written policies. This meant that guidance on disaster management for CBIS was inadequate in these institutions.

viii. Training: Training on disaster management for CBIS was not carried out by majority of the libraries studied. Only one institution carried out sensitization workshops to all its employees. Lack of structured programmes to guide on training, therefore, hampered skills transfer as well as creating awareness to employees on matters pertaining to disaster management for CBIS.

ix. Funding: All the target libraries reported lack of adequate funding to meet the needs of ICT infrastructure and activities. Thus, necessary equipment and measures to ensure disaster management for CBIS were hampered.

x. Top management of the organizations: Majority of the respondents indicated that the top management lacked awareness on issues pertaining to disaster management on CBIS. This influenced funding, staffing and support for the same.

xi. Employment procedures and terms of service: In all the target libraries, the employment procedures and terms of service for ICT personnel were a challenge. It was not possible to attract adequate and qualified ICT personnel.

xii. User population: User population increased the incidences of vandalism, theft and congestion of the internet connections.

xiii. Size and nature of the library building. A number of respondents indicated that size of the library building was big and, therefore, adequate surveillance was not possible. Also, some library buildings were constructed without consulting the ICT personnel whereby essential ICT facilities were not factored for in the building. Providing ICT services and facilities in such buildings became a challenge.

5.3 Conclusion

i. Libraries had taken some measures to prepare and mitigate disaster that could affect CBIS. The measures taken were in line with what had already been identified and which caused threats to CBIS such as vandalism, theft, virus attacks and software downloads. Since no major disaster affecting CBIS had occurred in libraries, the institutions had not invested heavily in disaster management infrastructure such as establishment of a functional data recovery centre.

ii. There were no disaster management teams in any of the institutions studied. This meant that disaster recovery for CBIS had not taken a centre stage in the organization's priority issues. This may have been due to lack of awareness by top management of the issues pertaining to disaster management. It could also have been due to the fact that no major disaster had occurred affecting the CBIS in the institutions studied.

iii. Lack of awareness by top management on disaster issues affecting CBIS may have had an effect on the establishment of disaster management policies, programmes and plans. Majority of the

institution studied lacked these very important documents that guide on day-to-day running of the organisation.

iv. Knowledge, skills and training normally have direct correlation with the performance of one's duties. Right training, skills and knowledge on CBIS influenced positively the way ICT issues were handled by the personnel involved. Lack these qualities with regard to CBIS had a negative effect on disaster mitigation and preparedness.

v. ICT field is very dynamic and it is virtually impossible to be fully prepared for disaster at any one particular time. The personnel involved, therefore, need to be aware that a disaster could occur unannounced. Hence, measures to ensure a high level of recovery should be put in place.

vi. Disaster management of CBIS in libraries calls for a multi departmental co-operation if it is to succeed.

vii. Training of users of CBIS is paramount to ensure the degree of protection and preparedness.

5.4 Recommendations

From the study findings, the researcher recommends the following:

5.4.1 Education and Training

The institutions' training library and information professionals at tertiary colleges and universities should do the following:

i. Incorporate practically-based IT courses in their curriculums to equip the library professionals with ICT skills and knowledge.

ii. Library and information science departments should co-operate with the ICT department in their institutions whereby the information professionals take ICT courses as part of their diploma or degree course.

iii. The library and information science department should have ICT specialization as one area that the students should take during the last two years of their courses. They should take IT as the core area and the library and information science as the auxiliary units.

iv. The students could also be exposed to the ICT environment during their attachment which normally takes 3 months. This should involve their attachment to an IT industry or ICT department to gain practical skills in ICT related issues.

v. Training and retraining of ISL to equip them with the necessary ICT skills and knowledge: Short courses on ICT can be taken by the ISL even if it is at a diploma level rather than employing ICTT under the ISL which brings confusion at times. This could also be done through a series of workshops and seminars which focus on IT and in particular security of CBIS. This will equip staff handling ICT activities on matters of security for CBIS.

5.4.2 Staffing

The institutions should be able to hire, retain, and retrain adequate qualified ICT personnel to handle ICT-related duties. To ensure this, the following should be done:

i. Remunerate ICT personnel accordingly to ensure they do not keep looking for greener pastures.

ii. Training and retraining: This will ensure that staff are updated with current knowledge and skills relating to security of CBIS.

iii. Provide adequate funds for training and retraining.

iv. Terms of service for ICT personnel should be improved and their career development be defined within the organizations.

5.4.3 Policies, Programmes and Plans

Policies to guide on the following aspects should be developed:

i. Usernames and passwords.

ii. Rights and privileges.

iii. Disaster recovery procedures.

iv. Training of users on disaster management of CBIS.

v. Employment of ICT personnel.

vi. Transitional termination of employment to ensure proper handing over.

5.4.4 Data Recovery Centres

Establish disaster recovery centres and develop DR plans. Any organization that is committed to ensuring security of their CBIS should develop DR centre as well as establish disaster recovery plans that will guide the organization in times of disaster. The plans should also list the disaster recovery teams and their responsibilities.

5.4.5 Co-operation and Partnership with Other Universities

Universities and libraries can cooperate or partner with other universities at both national and international levels. Most universities have projects that run in partnership with international universities and the issue of backing up data could be one of them. This could be on the following:

i. Hosting data recovery centres.

ii. Storage of data backup.

iii. Training of personnel on disaster management.

5.4.6 Partnership with other stakeholders

Universities and libraries could partner with other stakeholders to ensure backup of data and equipment. The stakeholders include the following:

i. Insurance companies to insure equipment and data.

ii. Data recovery organizations to establish and host data recovery centres.

iii. Vendors and suppliers of equipment and computing facilities to ensure availability of equipment in case of malfunction, vandalism or theft.

iv. Service providers such as Safaricom, KENET, ISPs, to ensure internet connectivity and other services.

5.4.7 Explore Other Methods of Ensuring Security of Data and Equipments

Other services currently being employed to ensure security of data and equipment include the following:

i. N-Computing: This will curb the problem of vandalism and illegal installation of software into the library computers.

ii. Cloud computing: To backup data on the cloud which ensures availability of data anytime and anywhere.

5.4.8 Policies at National Level

Relevant Ministries and institutions should come up with policies for the development of ICT infrastructure in educational institutions For example:

i. Ministry of ICT and Ministry of Education Science and Technology.

ii. Commission for University Education (CUE).

iii. Kenya Education Network (KENET).

5.4.9 Funds

Adequate funds should be availed for the following:

i. Equipment and other facilities.

ii. DR centres.

iii. Modern libraries.

iv. Insurance cover (for equipment and other facilities)

v. Education, training and retraining.

vi. Staffing.

5.4.10 Establishment of ICT Committees

Disaster recovery committees comprising of top management of the institution to discuss ICT related issues. This will create awareness for the top management and, therefore, make them more responsive to the needs of the ICT directorate.

5.5 Recommendations for Further Research

i. Technology plays a role in enhancing security. Therefore, research should be carried out on ways in which this could be used to enhance security of the CBIS.

ii. A study should also be done on business continuity planning in relation to CBIS to determine the level of preparedness by the university libraries in Kenya.

REFERENCES

Aziagola, P. C. and Edet, G. T. (2008). Disaster-control planning for academic libraries in West Africa. The *Journal of Academic Librarianship, vol. 34, no.3, p*. 265-268.

Bak, N. (2004). *Completing your thesis: A practicle guide*. Pretoria: Van Schaik Publisher.

Bordens, K. S. (1996). *Research Design and Methods: a process approach.* London: Mayfiel Publishing Company.

Boss, R. W. (2006). *Disaster planning for computers and networks*. PLA Tech Note: American. Library Association.

Caelli, W., Longley, D., Shain, M. (1991), Information Security Handbook, Macmillan, London,

Casper, S. (1998). Hands on instruction across the miles: using a web tutorial to teach the literature review process. *Research strategies, vol.16, No*. 3.

Cerullo, M.J., McDuffie, R.S. and Smith, L.M. (1994). Planning for disaster. *The CPA Journal, June, pp. 34-8.*

Cervone, H. Frank (2006). Disaster recovery and continuity planning for digital library systems. *OCLC systems & Services: International digital library perspectives, vol.22. no.3*. p173-178.

Chacha, N. C. (2005). *Reforming Higher Education in Kenya: challenges, lessons and opportunities*. IUCEA.

Chow, W.S. (2000). Success factors for IS disaster recovery planning in Hong Kong. *Information Management & Computer Security, Vol. 8 No. 2, pp. 80-6.*

Chow, W. S and Ha, W. O. (2009). Determinants of the critical success factors of disaster recovery planning for information Systems. *International Management & Computer Security, Vol. 17, no.*3. *p*.248-275.

Computer Based National Information Systems: *Technology and Public issues,*
2004.

Creswell, John W. (2009). *Research design: qualitative, quantitative and mixed methods approaches*. 3rd Ed. Los Angeles: Sage Publications.

Davies, H., Walters, M. (1998). Do all crises have to become disasters? Risk and risk mitigation. *Disaster Prevention and Management: An International Journal, Vol. 7 No.5, pp.396-400.*

Elstien, C. (1999). Reliance on technology. Enterprise Systems Journal, July, pp. 38-40. Feather, J. and Sturges, P. (eds) (2003). *International Encyclopedia of information and library science*, 2nd Ed. London: Routledge.

Federal Financial Institutions Examination Council (2006). Information Security
Booklet. *OCC BULLETIN 2006-31*

Fitgerald, J and Dennis, A. (2002). *Business data communications and networks.* 7th Ed. New York: John Wiley and Sons.

Forcht, K. A., Pierson, J. (1994), New technologies and future trends in computer security. *Industrial Management & Data Systems, Vol. 94 No.8, pp.30-6.*

Gay, L. R , Mills, G E., & Airrasian, P. (2009). *Educational research: competencies for analysis and applications*. London: Pearson Education.

Ginn, R.D. (1989). The case for continuity. Security Management, January, pp. 84-90. Glense, C. (2006*). Becoming qualitative researchers; an introduction*. 3rd Ed. Boston:.Pearson Education.

Hawkins, S. (2000). Disaster recovery planning; a strategy for data security. *Information Management & Computer security* 8/5, p.222-229.

Israel , M., and Hay. L (2006). *Research ethics for social scientists: between ethical conduct and regulatory compliance.* London: Sage.

Kaur, T (2009). Disaster planning in University Libraries in India: a neglected area. *New Library World, vol. 110, no*. 3/4, p. 175-187.

Kebede, G. (2002). *Modelling the information needs of users in the electronic information environment*. Phd. Thesis. University of Pietermaritzburg: University of Natal.

Kelly C. (1998), "Simplifying Disasters: Developing a model for Complex Non-linear Events". Proceedings of International Conference on Disaster Management: Crisis and Opportunity: *Hazard Management and Disaster Preparedness in Australasia and the Pacific Region, Cairns, Queensland, Australia*, p. 25-28, 1-4 November, 1998.

Khalid, Manmood. (1999) . The development of computerized library services in Pakistan: a review of literature. *Asian libraries. Vol. 8. No 9*. P. 307-328.

Kibaru, F. N .(2005). *Disaster recovery planning for business continuity in information systems; a survey of some organisastions in Nairobi*, Kenya. Msc Project. ICS UoN, Kenya.

Kimani, G. and Muthembwa, K. M. (1998). Disaster management (prevention). How well are Kenyan information managers prepared? Nairobi: SCESCAL.

Kimberly A. (2003), "Disaster Preparedness in Virginia Hospital Centre-Arlington after Sept 11, 2001" *Disaster Management and Response* 1(3): p. 80-86.

Klein, H. K and Joseph, P. A. (2007). *Information technology disaster planning: lessons learned from Katrina.* Proc. ISECON, V24.

Kochtanek, T. R & Matthews, J. R. (2004). *Library information systems: from library automation to distributed information access solutions*. New Jersey: Libraries Unlimited.

Kombo, D. K. and Tromp, D.L.A (2006). *Proposal and thesis writing: an introduction*. Nairobi: Paulines Publication Africa.

Kothari, C . R. (1985). *Research methodology: methods and techniques*, 2nd Ed. New Delhi: Wishwa Prakashan.

Kritzinger, E. (2006). Information security in an e-learning environment, 345-349. In *IFIP nineteenth World Computer Congress Education for the 21st Century*, pp. 345-349.

Kundu, S. C. (2004). Impact of computer disasters on information management: a study. *Industrial Management and data systems. Vol. 104. No*. 2.p. 136-143.

Laudon & Laudon (2000*).Management information systems: organization and technology in a networked enterprise.* 6 th Ed..New Jersey, Prentice-Hall.

Loch, K. D, Houston, H. C and Warkentin, M. E (1992). Threats to Information systems: today's reality, yesterday's understanding. *MIS Quartelly, vol. 16. No*.2 (Jun, 1999), p. 173-186.

Lyons, K. (2005). How to conduct a literature review. Available at : http:// www.library.ucsc.edu/ref/howto/literaturereview.html (accessed on 20th October, 2008).

Manitoba Health (2002). Disaster management model for the health sector; guideline for programme development. Version 1, November 2002.

Matthews, G and Eden P (1997). Disaster management in libraries. *Facilities, Vol. 15 Issue: 1/2, pp.42 – 49*

Maxwell, J.A (1992). Understanding and validity in qualitative research. *Harvard Educational Review, 62(3), pp. 279-300.*

McLntyre, J. (1998). Disaster control planning. Paper presented to the Annual Conference of the UK Serials Group, Leeds, 28-31 March 1998. *Serials Vol.1 No.2, July* 1998.

McNurlin, B.C. (1988). Trends in disaster. *I/S Analyzer, Vol. 26 No. 11, pp. 1-12.*

Meckler, P. (1991). A brief history of library automation: 1930-1996. London: Management issues and future perspectives.

Miles, M. B and Huberman, M. A. (1994). *Qualitative data analysis.* 2nd Ed.. Available at http://writing.colostate.edu/guides/research/observe/com2d4.cfm accessed 21 September, 2008)

Mugenda, O. and Mugenda , A. (1999). Research Methods: quantitative and qualitative approaches. Nairobi: African Centre for Technology studies (ACTS).

Ndungú C. (2002). A framework for development of an information security auditing capability. Msc project ICS-UoN, Kenya.

Nyandiere, C. (2007). Increasing role of computer-based information systems in the management of higher education institutions. Proceedings of the Seventh Annual Conference. Strathmore University Press. Nairobi. Kenya.

Oliver, M. (2004). Assessing and enhancing quality using toolkits. *Quality assuarance in Education Journal*, vol. 8. No. 1. p. 33-37.

Oliver, P. (2004). Writing your thesis. New Delhi: Vistar Publication.

Oso, W. Y. and Onen, D. (2005). A general guide to writing research proposal and report: a handbook for beginning researchers. Kisumu, Kenya : Options Press and Publisher.

Rohde, R. and Haskett, J. (1990). Disaster recovery planning for academic computing centers.*Communications of the ACM, Vol. 33 No. 6, pp. 652-7.*

Rothstein, P.J. (1998). Disaster recovery: in the line of fire. *Managing Office Technology, May,pp. 26-30.*

Rutherford, K. and Myer, G. (2000). Business continuity: do you have a plan? *Canadian Underwriter, April, pp. 38-41.*

Sauders, M, Lewis, P and Thornhill A. (2003). Research Methods for Business student. England: Pearson Education.

Sekeran, U (2003). Research methods for business: a skill building approach. New York: John Wiley and Sons.

Shaluf, I. (2007). Disaster types. *Disaster prevention and manangment*. Vol. 16. No.5 p704-717.

Stockburger, D (2004). Introductory statistics, concepts models and applications models . available., http://www. Psychstat.missouristate.edu/introbook/sbk04m.htm>6 accessed . 20th September , 2008.

Tran, S (2006). Security Information Management Challenges and Solutions. Accessed from http:// security information management challenges and solutions.html on 8th November 2011.

Turner B. A. (1994). "The organizational and Inter-organizational Development of Disasters" *Administrative Science Quarterly* 21: p. 379-397.

Wambiri, D. (2008). Disaster planning and Preparedness in University Libraries in Kenya. PhD Thesis. School of Information Science. Moi University, Eldoret, Kenya.

Wepman, J. (2010). Advantages of computer-based information systems. http://www.ehow.com/list_6748808_advantages_based-information-systems.html. accessed 8th January 2011.

Wheatman, V. (2001). Aftermath: disaster recovery. *Gartner Research*, AV-14-
5238

Wong, B.K., Monaco, J.A. and Sellaro, C.L. (1994). Disaster recovery planning: suggestions to top management and information systems managers. *Journal of Systems Management, May, pp. 28-32.*

Wong, L . (2006). Disaster planning in Libraries. *Journal of access services, vol.* 4, issue 3.4 p.71-82.

Zikmund, W. G. (2003). Business research methods. Ohio: Thomson

APPENDIX A: OBSERVATION GUIDE

The observation guide was used to collect information on observable measures that had been used by the libraries to prepare and mitigate for disaster that may affect computer-based information systems.

1. Presence of policies, disaster management plans, security policies, etc.

2. In the Server and computer rooms, assess the following:
    a. Ventilation
    b. Air conditioning
    c. Eating of foods and drinks
    d. Doors
    e. Alarm system
    f. Presence of CCTV
    g. Backups (Power backup)
    h. Existence of back up servers (s)
    i. Dust accumulation
    j. Location of the backup server and other computing equipments
    k. Authorization to the room

3. Use of guards at the entrance of the computer rooms

4. Use of lock and key for computers and computer rooms

5. Clocking in the computer rooms

6. Use of passwords (computer access authorization)

7. Use of biometrics or cards for authorization.

8. Presence of CCTVs in the library.

APPENDIX B: INTERVIEW GUIDE

UNIVERSITY LIBRARIAN / DEPUTY UNIVERSITY LIBRARIAN

Date_____

The interview guide was used to collect information from the University Librarian on issues pertaining to disaster preparedness and mitigation for computer-based information systems in libraries.

1. I introduced myself and explained the purpose of the interview
2. I explained the purpose of the research.
3. I asked the interviewee to briefly introduce oneself.

Gender : Male ☐ Female ☐

Age: Below 30years ☐ 31-40years ☐

41-50years ☐ Above 50Years ☐

Qualifications: Ph.D ☐ Masters Degree ☐

Bachelors Degree ☐ Diploma and Certificate ☐

Interview questions

1. Have you worked in another library?
2. How long have you worked in this institution?
3. Briefly tell me about your library.
4. Which electronic resources does the library have?
5. Does the library have computers or multimedia room?
6. What online services does the library offer to users such as Online Public Access Catalogue, e-journal access?
7. In your opinion what is computer-based information systems?
8. Has the library experienced any problem with its computer-based information systems?
   Yes No

   a. If yes, of what were they?
   b. How did it affect the operations of the library?
   c. How did the library deal with it?
   d. Who were involved in solving the problem?

e. What were the main challenges in your efforts to solve the problems encountered?
f. What measures has the library put in place to eliminate or reduce the occurrence of such problems?

9. If the library has not experienced any problem affecting its computer-based information systems, what has contributed to this success?

10. How does the library ensure that its resources are secure?

11. How does the library ensure security of its computer-based information systems?

12. In your opinion, what role does the university management play in disaster management for the CBIS in the library (Budget, policies, programmes, strategic plan, training?

13. What personnel are in-charge of disaster management in the organization?

14. Do they have defined roles and responsibilities?

15. What policies and programmes does the university have that focus on disaster management?

16. Does the library have any programmes, policies that focus on disaster management for computer-based information systems?
    a. If yes, which one are they?
    b. Who developed them?
    c. Are they approved?
    d. If yes, how often are they updated?
    e. Who updates them?
    f. Are the members of the library sensitized on the content of the programmes?
    g. If yes, when, how and by whom?

17. What policies and programmes does the library have that focus on disaster management?

18. What are the challenges or hindrances encountered in ensuring security for CBIS in the library?

19. What disaster(s) have you experienced in the library?

20. What is the role of information systems librarian as it relates to the security for CBIS?

21. Any other thing you may wish to add in regard to this study is welcome.

APPENDIX C: INTERVIEW GUIDE

INFORMATION SYSTEMS LIBRARIAN AND IT MANAGER

Date_____

The interview guide was used to collect information from the Information Systems Librarians and ICT managers on issues pertaining to disaster preparedness and mitigation for computer-based information systems in libraries.

1. I introduced myself

2. I explained the purpose of the interview to the interviewee.

3. I asked the interviewee to kindly introduce oneself

Gender: Male ☐ Female ☐

Age: Below 30years ☐ 31-40years ☐

41-50years ☐ Above 50Years ☐

Qualifications: Ph.D ☐ Masters Degree ☐

Bachelors Degree ☐ Diploma and Certificate ☐

Interview questions

1. Have you worked in another library?

2. How long have you worked in this institution?

3. In your opinion what does security for CBIS entail?

4. How does the library ensure security for its CBIS?

5. What measures has the library put in place to prevent disaster or disruption for CBIS?

6. In your own opinion, do you think your library is well prepared to handle disaster or any problem that might affect its CBIS?

a. If so, how?
b. If no, why not?

7. What measures are in place to ensure security of the computer-based information systems? (Prevention and preparedness measures). Please explain.

8. Kindly explain the support given by the top management in-order to ensure security of CBIS?

9. Are there written policies and programmes available in the university that deal with CBIS?

a. If so, do you have them or are they accessible to you?
b. What do they address? Please explain.
c. Were you involved in developing them?
d. If yes, on what basis? What were your contributions?
e. If no, why not? Explain your answer.

10. Are there written policies and programmes that focus on security or disaster management for CBIS in the organisation?

a. If so, do you have them or are they accessible to you?
b. What do they address? Please explain.
c. Were you involved in developing them?
d. If yes, on what basis? What were your contributions?
e. If no, why not? Explain your answer.
f. Are they updated? If so when and by who?
g. If no, why not?
h. Are they tested approved?
i. If no, why not?

11. Are there written policies and programmes that focus on security or disaster management for CBIS in the library?

a. If so, do have them or are they accessible to you?
b. What do they address? Please explain.
c. Were you involved in developing them?
d. If yes, on what basis? What were your contributions?
e. If no, why not? Explain your answer
f. Are they updated? If so when and by who?
g. If no, why not?
h. If no, why not?

12. What role do you play in ensuring security of CBIS? Role in DM of CBIS?

13. Are they well defined in your contract?

14. Do you have any training focusing on DM?

a. If so, which one?
b. If not, do you think it is necessary to be trained on disaster management for CBIS?
c. If so, what have you done towards this goal?

15. Has the library experienced any security problem or disaster relating to CBIS?

a. If so, please explain the nature of the problem.How did you recover from the problem?

b. If not, do you think there is likelihood that the library will experience any security problem that may affect its CBIS? Please explain your answer.

16. What problems or challenges do you experience in your endeavor to ensure security for CBIS?

17. Does the library cooperate with the institutional IT manger/Director in ensuring security for CBIS in the library?

a. If so, in which ways does the library cooperate with the ICT directorate in the institution to ensure security for CBIS in the library? Please explain.

b. If not, why?

18. Who maintains library CBIS?

19. Any other information or question you may wish to add is most welcome.

APPENDIX D: INTERVIEW GUIDE

CIRCULATION LIBRARIAN

Date_____

The interview guide was used to collect information from Circulation Librarians on issues pertaining to disaster preparedness and mitigation for computer-based information systems in libraries.

1. I introduced myself

2. I explained the purpose of the interview to the interviewee.

3. I asked the interviewee to kindly introduce oneself

Gender : Male ☐ Female ☐

Age: Below 30years ☐ 31-40years ☐

41-50years ☐ Above 50Years ☐

Qualifications: Ph.D ☐ Masters Degree ☐

Bachelors Degree ☐ Diploma and Certificate ☐

Interview questions

1. Have you worked in another library?

2. How long have you worked in this institution?

3. In your opinion what is CBIS?

4. Does the library have a multimedia centre?

    a. If so, what is its importance in the library?
    b. If no, why not?

5. Does the library offer online services?

    a. If so, which ones?
    b. If no, why not?

6. Are there electronic resources in the library?

    a. If so, which ones?
    b. If no, why not?

7. In your opinion what does security for CBIS entail?
8. Has the library experienced a security problem or disaster relating to computer-based information systems?
    a. If so, explain.

   b. What effect did this have on the library operations and services?
   c. Are there times when the library was unable to recover from a disaster/problem?
   d. How did this affect the library?
   e. If no, why do you think this has been the case?

9. What are the major problems experienced by computer users in the library? Please explain.

10. In what ways does the top management play a role in the security for CBIS?

11. In your opinion what are the major challenges affecting security or disaster management of the CBIS in the library?

12. What measures has the library put in place to ensure security of CBIS?

13. Have you received any training targeting library staff on disaster management?
   a. If so, in what form?
   b. Was it sufficient or relevant?

APPENDIX E: DOCUMENTS ANALYSED

1. Policy documents relating to computer-based information systems
2. Disaster management plans relating to computer-based information systems
3. Strategic plans
4. Training programmes/documents
5. Rules and guidelines on the use of computers and computer rooms.

APPENDIX F: RESEARCH PERMIT

APPENDIX G: PhD AUTHORIZATION