Assessment of the Security Systems in Selected Libraries of Higher Learning Institutions in Zambia

By

Bestain Hampwaye

A dissertation submitted to the University of Zambia in partial fulfilment of the requirements for the award of the degree of Master of Library and Information Science (MLIS)

THE UNIVERSITY OF ZAMBIA

LUSAKA

2022

COPYRIGHT

DECLARATION

I, **Bestain Hampwaye** do hereby declare that this dissertation represents my work and that it has never been submitted by anyone at the University of Zambia or at any other University to acquire a diploma, degree, or any other qualification.

Signed: …….

Date: ……

CERTIFICATE OF APPROVAL

This dissertation of **Bastain Hampwaye** has been approved as a partial fulfilment of the requirements for the award of Master of Library and Information Science by the University of Zambia.

Name of Examiner	Signature	Date
……	……..	…..……..
……	…….	…….
……...	…….……	…….

Supervisors' Name	Signature	Date
……..	…….	…….
……..	……	……..

ABSTRACT

Security issues in libraries include theft of library materials, the mutilation or vandalism of library resources and dealing with disruptive patrons. Therefore, the purpose of this study was to investigate security measures implemented to prevent theft of library resources and other disruptive vices in selected libraries in Zambia. Specifically, the study investigated the types of security problems being faced by higher learning institutions libraries in Zambia; it also investigated security measures higher learning institutions libraries have put in place to mitigate against security problems libraries are facing and assessed the effectiveness of the security systems used by these libraries. An exploratory study approach was adopted for this study and employed the qualitative method. A purposive sampling technique was used to select the respondents. The data elements from selected academic libraries were the librarians'/deputy librarians, the information systems librarians/IT managers, and circulation librarians. There were 15 libraries under study and were drawn from three provinces; namely; Lusaka, Central and Copperbelt provinces. The sample included libraries drawn from both public and private higher institutions of learning. The basic criteria for selecting libraries was that the institutions should have fully established libraries manned by personnel with a minimum qualification of a Bachelor's degree in library studies (BALIS). A total of 28 participants took part in the study. The research data was collected using interview guides; an observation checklist and a list of documents were collected, while data was analyzed thematically. The study revealed significant differences among higher learning institutions libraries in Zambia in applying the organizational security measures due to several challenges such as lack of security policies, incompetent staff and inadequate funds for security systems. However, some libraries have put in place security measures to protect their resources which include the installation of surveillance cameras, alarm system, 3M book detection system, generators, training of library staff and the use of security guards to man higher learning institutions libraries. The findings further revealed that half of the higher learning institutions libraries surveyed have deployed technological security measures but require improvement on organizational measures and maintenance of the security devices. This may be due to the over-emphasis on technology as the sole solution to security problems in these libraries. Therefore, the study recommended that security officers should be employed as a security measure since relying on technology alone will not solve the security problems effectively.

Keywords: Library, security systems; library resources, security measures; information resources; Zambia

DEDICATION

I dictated this work to my family. This work was undertaken during the time I was going through hardships with my daughter Luyando Hampwaye who was not feeling well. I dedicate this to my wife Edith Habukali Hampwaye, and my children Luyando Hampwaye, Lubaya Hampwaye and Gift Choongo for their understanding when I needed to be away from home doing the same work. Finally, I dedicate this work to you my uncle Dr. Hampwaye Godfrey, for you has been my inspiration and pillar.

ACKNOWLEDGMENTS

I wish to express my sincere gratitude to several people who contributed to this document. I wish to thank Dr. Akakandelwa Akakandelwa and Dr. Kanyengo Christine Wamunyima for having guided me from the identification of the research topic up to the conclusion of the study. The progress of this dissertation saw the involvement of the Judiciary judges, lawyers (Research Advocates), and library staff. Without their involvement in providing data, this study would not have been a success. I also wish to thank my supervisor at work Mrs. Chitumbo for permitting me to attend classes during my first part of my masters' programme. Profound gratitude also goes to my family for their patience and sacrifice during my studies. Above all, I want to thank the Almighty God for his mercies and favour for the provision of the grace to accomplish my studies. To God be all the glory!!

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

AACR	Angro-America Cataloguing Rules.
ACRL	Association of Colleges and Research Libraries.
ALA	American Library Association.
CAIS	Computer Accounting Information System.
CARI	Cyprus Academic Research Institute.
CBIS	Computer Based Information System
CBU	Copperbelt University
CCTV	Closed Circuit Television.
CMS	Computer Management System
CSMM	Collection Security Management Model.
DDos	Distributed Denial of Services
DoS	Denial of Service.
GDTs	General Deterrence Theories.
ICT	Information and Communication Technology.
ICTs	Information and Communication Technologies.
ILL	Interlibrary Loan.
IP	Internet Protocol.
IS	Information System.
ISec	Information Security.
ISM	International System Management.
ISM	Information System Management.
IT	Information Technology.
KNUST	Kwame Nkurumah University of Science and Technology
LAMU	Lusaka Apex University
LAN	Local Area Network.
LIAZ	Library and Information Association of Zambia
MARC	Machine Readable Cataloguing.
MIS	Management Information System
MPS	Malaysian Public Service.
NACSIS	National Institute of Informatics.
NRDC	Natural Resource Development College.
OPACs	Online Public Access Catalogues

PKU	Peking University.
RFID	Radio Frequency Identification.
S. A	South Africa.
SADC	Southern Africa Development Community.
SMEs	Small and Medium Enterprises.
UCT	University Center for African Studies.
UK	United Kingdom.
UMLs	University of Malawi Library.
UNESCO	United Nations Educational Scientific and Cultural Organisation.
UNILAS	University of Lusaka.
UNRF	University of Nicosia Research Foundation.
UNZA	University of Zambia.
USA	United States of America.
USB	Universal Serial Bus.
VPN	Virtual Private Network.
WiFi	Wireless Fidelity
ZALICO	Zambia Library Consortium

CHAPTER ONE: INTRODUCTION

1.0 Overview

This chapter covers the background to the study, the statement of the problem, objectives of the study, research questions, justification and significance of the study, delimitation of the study, and theoretical and conceptual framework

1.1 Background of the Study

Libraries of higher institutions of learning have been recognized as the 'hearts' of the institutions to which they're attached (Ogunyade, 2005). These libraries of higher institutions of learning are situated within the institutions whose collections are basically for all the schools and departments within the institution. To fulfill their mission of supporting the academic objectives of their parent bodies, which include teaching, learning, research, and cultural development, libraries develop and maintain standard books, journals, and audio-visual collections. Further, they provide services like free computer use, internet access, WiFi, and research support.

Ogunsola (2006), observes that the supply of up-to-date and effective library collections in higher learning institutions libraries is taken into account as a big function for supporting teaching, learning, and research. These services constitute the bedrock for services provided to the community. A library is the hallmark of each learning environment; it is the knowledge powerhouse that creates a behavioural study lifetime of students and lecturers to perfect their educational life. Hence, libraries are valued by their collection size (Ogunsola, 2006).

According to Choy (2007), libraries of higher institutions of learning assume a focus where users of diversified age groups, socio-political, economic backgrounds, and cultural interests need to converge to use all the available materials that can meet their individual needs. Every library of a higher institution of learning that aims to satisfy the knowledge needs of academics and researchers must take care and manage its collection well (Choy, 2007). The gathering is a crucial component of the library because it is known to be the base upon which a library adds value and provides essential services to its users. Since ancient times, libraries have been determined by their collections. For some time, the usefulness of a library remained on dimensions and quality of its collection. Most of the works that libraries do are tied to their collections, (Choy, 2007). The protection of library collections has profound impact on library survival. Carey (2008) defines library

security as the arrangements provided for safe and secure of library resources such as library equipment, library staff and library users. Library security is important because it ensures that library collections such as books and non-book materials are protected against unauthorized removals and vandalism. This involves safety of books against theft, mutilation, fire outbreak, insects, flood and protection of the premises against intruders.

Library security is important in a library set up in order to prevent security problems such as stealing, mutilation and vandalism of library materials. There are a variety of other things that require to be protected which incorporates the personnel safety of the workers, customers; tangible property, like library books or print materials, equipment, and intangible property, like highly classified data or information from databases (Lavanya, 2017). The protection of persons and property against a broad range of hazards such as crime, fire, accidents, sabotage, and attack is very important for smooth running of libraries.

1.2 History of Library Security Globally

Abubakar and Aduku (2016) observed that one of the greatest problem that has bothered libraries from the earliest times to the present is how to ensure security of library materials against theft and mutilation and vandalism. In earliest libraries security of library materials was purely traditional, particularly before the genesis of the printing press. In the ancient times books had chains on them to prevent against theft. Maidabino **(**2010) stated that in ancient Egypt, the writings on papyrus and leather were restricted to tombs and temple archive rooms under lock and key to prevent them from theft. He further asserted that protection of documents is a practice with long history. It was also revealed that parchment and clay tablets in ancient Middle East and in the middle ages of Europe chained-locked materials as some of the ways that was put in place to safeguard library resources from theft and vandalism. Within the library room records were mostly stored using pigeonhole niches in the walls. The use of open wooden or clay shelves was common which were lining the walls and the container system which was using wooden or brick boxes, woven reed baskets or leather containers is evident enough that ancient libraries prevented their materials from being abused (Maidabino. 2010).

The security of ancient libraries is old on its own way. Therefore, the question that need an answer is that can security of ancient libraries and their features be of practical use in today's libraries of higher institutions of learning. It is important to note that library security has progressed tremendously. The history of library security has shown some of the ways in which

the practices of ancient libraries mirror some of the features we see today in the modern libraries (Casson, 2001).

According to Rajendran and Rathinasabapathy,(2007) library of Agene in Babylonian had devised procedure in which users was requested to write down the number of the tablet that was required and give the list to the librarian who would then retrieve the needed materials from the collection. Clay labels were found each with a small opening or hole through which a wire could be threaded to avoid unauthorized removal. In order to prevent materials from theft these libraries used both the cylinder and stamp seal to identify tablets in the collections of the library. The doorless and windowless archive room" which could be entered "by ladder from above, in which tablets were stored" and the owner of the works had the fourth (series) of them to hand, had lost the third tablet and kept the first two in the less accessible archive room, making it necessary to list their contents for reference". This shows that these libraries had put in place some security measures to prevent loss of their collections (Rajendran and Rathinasabapathy, 2007).

Library security problem has been an issue before the begginning of printing press, by then manuscripts and books were written using hands (Rajendran and Rathinasabapathy, 2007). After books were written a curse were put in each and every book to prevent theft of these materials. The following are some of the good examples of the curses that were put in books. For him that stealth a book from the library; let it change into a Serpent in his hand and rend him; let him be struck with Palsy and all his members blasted; let him languish in Pain crying aloud for Mercy; let there be no Surcease in his Agony till he sinks to Dissolution; let bookworms gnaw his entrails in token of the Worm that dieth not, When at least he goeth to his final Punishment; let the flames of hell consume him forever and aye; Steal not this Book my honest Friend; For fear the gallows should be your hend; And when you die the Lord will say; And wares the Book you stole away? Casson, (2001) stated that threats and curses that were put in books can be referred to overdue and fines notices of today. This is where Ashurbanipal declared, ‘’whoever removes the tablet, writes his name in place of my name, may Ashur and Ninlil cast him down, erase his name, his seed and in the land’’(Casson, 2001).

The above letters were written and attached to every book in the library to scare patrons from removing books illegally without due process. In spite of these curses put in books in the medieval times, these materials continued missing. During the ancient time books were chained and were put on the guard to prevent them from theft. Despite putting these measures in place

loss of materials still persisted and up to now libraries have continued battling with security issues (Rajendran & Rathinasabapathy, 2007).

Vellani (2010) stated that early libraries were very conscious of security of their library materials as evidenced from the various security methods employed such as chaining and locking of library materials. He further said that some of the security methods have continued to be adopted in present day libraries, others have been modernised, with technological advancement opening new frontiers for preservation and security of information resources and services in the numerous libraries of higher institutions of learning.

1.3 Context of the Study

It has been shown from the introduction that the coming and use of sophisticated technology in libraries to provide safety of library resources have over the years spread around the global Person (2007). However, many libraries in developing countries have been struggling to purchase the important gadgets due to so many factors such as inadequate funds, the high cost of modern technology, high maintenance cost and lack of expertise to run them. In most cases, libraries tend to hire people for installation and maintenance of these equipment.

The modern technology has also come with some challenges when providing security to library materials as they need to be incorporated with other characters for them to work effectively and reduce security threats. According to (UNESCO, 2015), sometime back, libraries entirely depended on manual security physical check by the security guards while electronic devices performs basic functions. With the development of technologies, the use of electronic security systems is considered as the best way of resolving library security problems (Cannaway & Powel, 2010).

Like many other libraries in higher learning institutions in Zambia, most of the libraries have failed to embrace modern technologies in Zambia. The use of electronic security systems in most institutions of higher learning is very low as they largely depend on physical security (Simukali, 2019). For example, the University of Zambia library before then lost library materials due to lack adequate security systems, disaster preparedness and recovery plans (Shameenda, 2011).

However, in order to improve security awareness to library resources most libraries of higher education institutions have been training their staff. The main aim is to increase security awareness to staff and library users as this plays a critical role in protecting library resources

from being abused (Halubanza, Kunda & Musonda, 2021). The trainings are also important because they highlight the consequences to those who are to be found wanting.

1.4 Statement of the Problem

Libraries are the bedrock of higher institutions of learning which are required to ensure availability library resources at a time they are needed. Their mandate is to support teaching, research, cultural and community service. These libraries are known to be the information hubs of the learning community, empowering students, and faculty to learn, do research, and advance the frontiers of knowledge.

Libraries have been spending a lot of money when buying books and other needed materials for their normal operations. It is also important to note that prices of books and other materials have continued to rise, forcing many libraries to reduce or completely cancel the subscription and purchase of library materials. Libraries of higher institutions of learning in Zambia have been also continuously spending huge sums of money replacing stolen and damaged resources that are acquired through hardly earned money. Because of the financial difficulties libraries are facing there is a need to protect the acquired materials jealously. If this problem is not attended to libraries of higher education institutions of learning may render their role irrelevant, as in most cases, they fail to meet the knowledge needs of both the faculty staff and researchers in their respective fields. However, it is observed that over the years, many factors have been militating against the security of information resources in academic libraries (Ogunyade, 2005).

Studies have been conducted on security threats in many countries such as Nigeria, Ghana, UK, USA, India, France, Kenya, Malaysia and Australia Ogbonyomi, (2011); Osayande, (2009); Gupta & Sharman, 2008; Oyesiku, Buraimo, & Olusanya, (2012); AlHogail (2015); Haniza, 2009; Christopher & Sadat, (2014). These studies have tried highlight the security threats that libraries of higher learning institutions are facing and the measures that have been put in place to mitigate threats. However, most of the studies failed to consider the holistic approach to curb security challenges which libraries are facing. The studies should have failed to highlight the benefits that accrue through the use of these security measures of which they did not. For example**,** studies done by Isebe, (2014), Salaam and Onifade, (2010) concentrated on why students mutilate print materials. The studies highlighted the causes of why students abuse library materials. The scholars did not look at all possible threats to library materials such as intruders, library staff and fire just to mention a few.

Ogbonyomi (2011), Osayande (2009), Abioye and Adeowu,(2013) in their studies observed that threats to information resources in the library include theft, mutilation, hiding, other disruptive acts, and bad attitudes towards library collections and these led to depletion of library materials. But the authors did not go deeper to explain how best to resolve the problems which libraries are facing. Therefore, there was need to carry out this study in the Zambian context in order to find precise measure to security issues and the security measures put in place. Further, to find out the reason for adopting such measures, the benefits they have brought to libraries and as well to find out the challenges which libraries are facing when using them. It is on this premise that this study interests to investigate the security measures adopted to prevent theft of library resources in selected libraries in Zambia.

1.5 Purpose of the Study

The purpose of this study was to establish more about the security measures that were put in place to reduce the various threats that are common in higher learning institutions libraries such as theft and vandalism of library materials. The study further sought to determine the impact of these security measures put in place on security issues in libraries. The study also sought to know the anticipated potential benefits that have accrued to libraries that have adopted the security measures. There are a number of benefits attached to the use of security measures as they prevent theft and vandalism of library resources. Therefore, it was important to determine the benefits that comes with adoption of these security measures by libraries of higher institutions of learning in Zambia. It must be also noted that the adoption and use of these security measures come with some challenges and it was the purpose of this study know the challenges that libraries face. The identification of the challenges helps in finding effective security measures to library materials.

1.6 Objective of the Study

The main objective of this study is to investigate security measures adopted to prevent theft of library resources in selected academic libraries in Zambia. The specific objectives of this study were to:

i. establish the types of security problems being faced by academic libraries in Zambia.
ii. establish security measures academic libraries have put in place to mitigate against security problems libraries are facing.

iii. determine the effectiveness of the security systems used by academic libraries understudy.

1.7 Research Questions

The study was directed by the following research questions:

i. What types of security problems faced by academic libraries in Zambia?
ii. What are the security measures academic libraries have put in place to mitigate against security problem they face?
iii. How effective are the security measures put in place by libraries of higher institutions of learning understudy?

1.8 Significance of the Study

Libraries in higher learning institutions in many countries are not always safe and secure as they have been experiencing loss and mutilation of print materials. It is reported that most libraries across the global are facing security problems to their resources. For example, in France (Clusif, 2008), Saudi and Abu-Musa, (2010), Kenya (Kimwele, Mwangi, and Kimani, 2005), Malaysia (Unisys, 2007) and Nigeria (Shamsul et al, 2012), a number of studies were conducted which led to the development literature on security challenges and measure adopted to prevent threats in libraries of higher education institutions. Many literatures have been published on security threats and measures to do with libraries. However, there is no study of this nature that has been conducted in Zambia to find out about security threats to library resources as well as measures that were put in place. The study by Shameenda (2011) only looked at the deployment of security guards and surveillance cameras in the University of Zambia Library and did not cast the net widely to other libraries. It was therefore, necessary to conduct a study that could cover a number of libraries in detail. This could help to know the security threats of which libraries are facing and also the security measures that were put in place

Since there has been no research on this matter to measure the depth of security issues and the measures that has been put in place in Zambia. The findings will help to provide solutions to security problems libraries are facing. It is hoped that the findings of this study may help policymakers to intervene to come up with better ways of providing security to library materials in Zambia. The study may also help stakeholders involved in librarianship such as Zambia Library Consortium (ZALICO), and Library and Information Association

of Zambia (LIAZ) to influence policy formulation on library security issues. The findings of the study have shown that a lot of libraries do not have security policies in place.

This study will help to develop an integrated approach to handling security problems with libraries. This is based on the need to improve the security of library materials in order to prevent book thefts of libraries of higher learning institutions in Zambia, especially that it relates well to the research and also re-examine the roles of the libraries of higher learning institutions in order to achieve the objectives of the study. The negative effects on the security of library materials affects the effective provision of adequate information materials to library users. The study further highlighted the challenge being faced by libraries such as inadequate funding. The budget allocation to purchase library resources is very difficult, especially during this period of economic depression. The study of this kind becomes very important in order to understand various lapses in the security of library materials so as to elongate lifespan of library resources and reduce the cost of repairs and replacement of these materials.

The findings of the study may also help library administrators to understand the importance of installing security systems in libraries. The improvement of security systems will provide academic libraries with an opportunity to meet user's information need as this will reduce mutilation and theft of library materials. The results of the study may also assist library staff to be trained or made aware of security issues and ensure that they are affected. Above all the collected information will contribute to the already existing body of knowledge. The factual information might also assist in justification as to why there must be an increase in funding libraries in Zambia.

1.9 Limitations

The major limiting factor is that the study is merely restricted to a few academic libraries because of limited time and financial constraints. It should be also mentioned that not all provinces were included in the study. The libraries under study are largely situated in Lusaka, Central and Copperbelt provinces because that's where an enormous concentration of the targeted population might be found. As a result, the findings of the study cannot be considered to be the same with other libraries in Zambia. However, certain experiences could be of benefit to other libraries within the country. Another problem is that the researcher did not collect all the required information from all the respondents because of other commitments. Other key informants targeted for the

research were not reached because of their busy schedules and also because of time and financial constraints rescheduling of appointments may be a problem for the researcher. However, the limitations were resolved by conducting telephone interviews since it was not possible to meet them physically.

1.10 Scope of the Study

Although there are many libraries of higher institutions of learning in Zambia, the study was delimited to only to the University of Zambia (UNZA), Kwame-Nkrumah University, Zambia Open University, Zambia Centre of Accountancy, Evelyn Hone College, Natural Resources Development College (NRDC), University of Lusaka (UNILAS), Lusaka Business and Technical College, St Eugene University, Chalimbana University, Copperbelt University (CBU), Chainama College, Justo Mwale Theological University, Lusaka Apex Medical University (LAMU) and Mulungushi University. The study looked at the security issues libraries face such as theft of library resources and the common security measures put in place in various libraries of higher learning institutions as well as the effectiveness of the security measures.

1.11 Theoretical Framework

The study adopted the operational model theory referred to as House Security Management Model proposed by Da Veiga and Eloff (2007). According to the House Security Management Model, factors that comprise collection security management in libraries are derived from published literature. The factors are then put in a "house" for security management as it is in libraries. The house adopts and adapts the operational model proposed by Da Veiga and Eloff (2007), who has used a house to border the knowledge system security governance. The model compares a library collection security governance to a secured house where the alarm installed provides adequate protection. Nevertheless, even during this secure situation, security could also be breached if the owner leaves the house with the front entrance unlocked. This explains that security measures could be ineffective if the behavior of the people within the home or in a corporation is unconcerned about implementing the safety processes. The model is viewed from five factors such as governance, operational processes, people awareness and training, physical and technological perspectives, and security culture. The framework must provide management with a working instrument to assess and implement a more holistic approach to the security management of library materials. This theory can be summarized in the following:

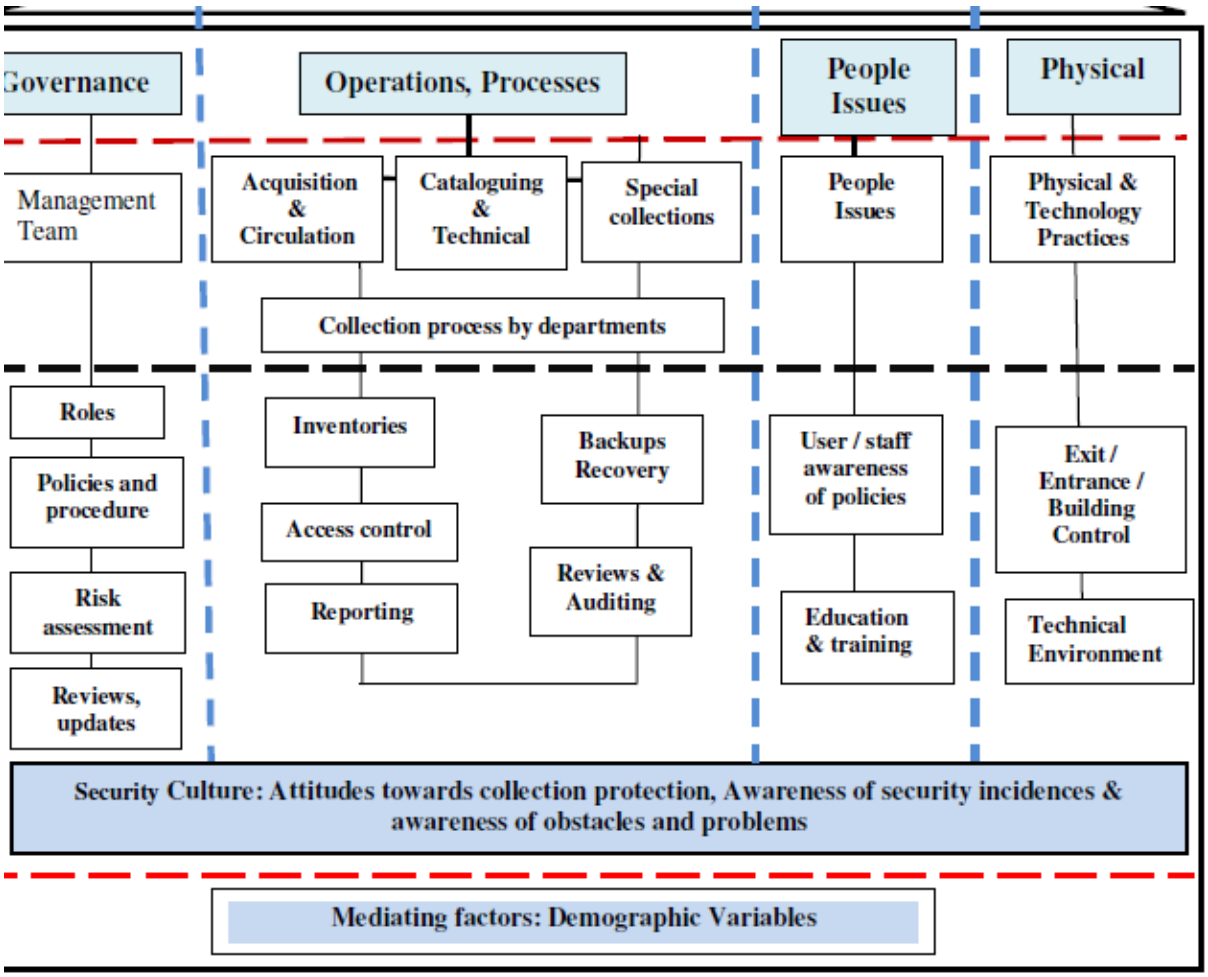

Figure 1: The House Security Management Model in Libraries.

Constructs in the house security model provides the following:

Integrity, the library has to make sure that the collection or the information they carry is not altered, accurate and complete. Therefore, management of the collection requires protection from accidental or deliberate change of the contents. Accuracy refers to proper description of collections, which are shelved or stored appropriately. Completeness refer to collections that are not mutilated, missing, decayed, misplaced, over borrowed, protected from deliberate or accidental change, and secure from vandalism or theft.

Confidentiality, this refers that the collection is available only to those authorized at the various levels (controlled access to types of registered members).

Availability, this refer to making sure that authorised users have reliable and timely access to collection at the time they need it (timeliness) and at the promised times (appropriate opening hours) and through a reliable network system, which makes items available without delay. The model describes a holistic plan for collection protection in libraries, combining the governance, process, people, physical and cultural factors to ensure that a reasonable level of collection

security management is in place, hence minimizing risks to the library's main assets, its collections. In the model all factors are of equal weight in ensuring that the confidentiality, integrity and availability of the library's collections are maintained at a reasonable level.

1. 11.1 The Governance

In this context, governance means having a management team in the library that is to provide roles, policies, procedures, risk assessment and reviews updates. The members of a security team is responsible for formulating objectives. These security team is there to ensuring that objectives and policies are achieved and to ascertaining that risks are identified and managed appropriately (Allen & Westby, 2007). The governance factor stresses the importance of considering collection security as a part of management responsibility (Brown & Patkus, 2007). This simply means that libraries should design a compressed strategy with plans that persuasive the vision and direction for risk management (Purtell, 2007). The security management team ideally should be chaired by senior personnel with representation from various departments, and members from the security wing. The team members should have the required experience and knowledge about collection security issues and management so that they will command the authority to manage and ensure collection security compliance.

Cowan, (2003), argues that risk assessment is important to undertake to spot risks at various levels in the library setting so that security planning is prioritized. The Governance factor stresses the necessity for library and collection managers to document, maintain, review and update risk policies and procedures. They also prepare reports via newsletters, web pages, and other publications to announce collection security initiatives and also create awareness amongst employees and users (Saffady, 2005). This factor provides evidence about whether good collection security governance is in place in libraries or not.

1.11.2 The Operational Processes

This factor involves the processes of putting into operation security programs formulated by the safety management team through the relevant departments. These include the acquisition department, which is involved in accessioning and marking items to establish ownership, maintaining an inventory list which can be used to identify missing, misplaced or cost of things, and to facilitate backups and recovery processes (Holt, 2007); the circulation department, which shelves and stores items for quick and straight forward inspection by users, uses a manual or computer systems to record borrowed and

also to track the use of the collections, control access, undertaking stocktaking and inventory, report on disobedient borrowings, items that are lost, misplaced, abused, damaged, and stolen resources (Brown & Patkus, 2007). The cataloguing and technical department, which processes and record collections in the library's catalogue system, as well as attach identification marks to determine ownership and it as well ensure that the status of reporting materials that are not processed and access to such items is restricted (Brown & Patkus, 2007). The special collections are involved in preserving and conserving collections, controlling and monitoring access, proper inspection of the materials before and after use, and providing coverage for valuable library collections (Holt, 2007).

1.11.3 People Awareness and Training Programmes

This factor involves the human or people aspects of the model, especially programmes involving the training of staff, retrain and make deliberate policies and procedures on collection security management processes. This must comprise of security awareness formalized in organizational policy and procedures and it should be communicated to every library user and employee who works in the library (Saffady, 2005). It stipulates the necessity to work out collection security roles and responsibilities in university libraries and ways to handle, supervise, and monitor qualified and trained staff. Staff's knowledge of the supply of coaching programmes will help them handle security incidences, prepare reliable and useful reports.

1.11.4 Physical and Technology Factors

This factor involves both physical and technical mechanisms in implementing a secure environment in the library. The physical environment may be described as the safety and security of the library premises which holds library collections (Ameen, 2007). The physical security measures should begin with the physical architecture of the building or management of space where collections are held. It is also about controlling library entrances and exits, requiring identifications of access to general, rare and special collections areas. This as well require putting in place security patrols within the building parameters. The technical aspect consists of the technology practices and procedures that the collection security programmes embrace. This simply refers to the electronic security system and devices that are to handle collection security processes, control security threats, and install security systems at strategic entry points of the library. The security systems may include electronic gadgets such as anti-theft devices, visual cameras, smoke

detection, and alarm system at entrances, exits, and stack areas in the library. This system will help prevent unauthorized removal of library collections, monitoring, and detection of users in the reading and reference sections, as well as shelving areas (Ameen, 2007).

1.11.5. Security Culture

(Brown and Patkus, 2007) argue that this factor encompasses acceptable user and staff's attitudes and awareness toward the importance of protecting collections in the library. Awareness is an element that cannot be seen but it is demonstrated through perceptions such as staff's attitudes about the importance of security policies and processes, their awareness of security threats, and the limitations of implementations. Furthermore, Brown and Patkus, (2007) refer to this situation as a shared culture of mutual responsibility for security and safety where the staff is provided with the information and the tools to respond to some situations so that they can take action when called upon to do so. This attitude and awareness are grounds for the effectiveness of security governance, management, and operations. This is based on the premise that organizations do not change, but people change, and therefore it is people who are supposed to change the organizations (Brown & Patkus, 2007).

It can be argued that the model guarantee security of library materials if libraries in Zambia are to use the security measures properly. If the model is perceived effective and offer numerous advantages, many libraries in Zambia are likely to adopt the security measures so that they can prevent theft of their library resources.

1.12 Operational Definition of key Terms

(i) Libraries of Higher Learning Institutions: The library which is attached to an academic institution serving the teaching and research needs of staff and students (Otike & Barát,2021).

(ii) Library Security: It is deliberate or well planned designed security system to protect library resources against theft (Ajegbomogum, 2004).

(iii) Electronic Security System: Any method of preventing users from illegally removing library materials and the system relies on mechanical devices that detect when unauthorised library materials are being removed from the library (Osayande, Odaro, 2011).

(iv) Mutilation of Library Materials: The deliberate cutting up or vandalism of an item in the library collection (Omoike & Alabi, 2020). This can mean the cutting up of

material and remove part of it from the library collection. It can also mean damaging library materials so that other users may not use the material.

1. 13 Ethical Considerations

The researcher endeavoured to adhere to ethical code of conduct outlined by the Directorate of Research and Graduate Studies of the University of Zambia. First of all, a letter of introduction was obtained from directorate to facilitate the researcher's visits to selected libraries to conduct interviews. Further, participation of the participants in this study was done through informed consent. This means that participants were informed about the objectives of the study before interviews were conducted and those who were not willing to participate were not forced. Confidentiality was assured to respondents that agreed to participate and were informed that the information sought was purely for academic purposes. Furthermore, when coding and recording process real names were not used, the researcher disassociated names from responses. The interviews were only audio recorded with permission from the interviewees and those who declined, the interview was not recorded. The interpretation and presentation of the data collected was not doctored to suit the opinion of the researcher.

1.14 Summary of Chapter 1

This chapter provided the introduction, background of the study, statement of the matter, the objective of the study, specific objectives, research questions, significance of the study, theoretical framework to guide the study, definitions of terms utilized in the study, limitations of study and lastly ethical consideration. The research has revealed that libraries of higher institutions of higher learning globally are faced with a lot of problems concerning security of library resources such as theft, mutilation and vandalism. The study further established that these libraries have put in place some security measures to protect their library materials. The security measures that have been put in place to protect library resources include physical and technological. The physical measure starts with the physical architecture of the library building, the use of security guards to man the entrance and the exit of the library. The technological aspect is the installation of electronic gadgets in the library such as closed circuit television cameras CCTV, alarm systems to protect materials from theft. However, libraries are faced with financial difficulties to acquire electronic security systems because of inadequate funding libraries are receiving. Most of the studies failed to consider the holistic approach to mitigate security problems which libraries are facing. The house security management model was used in this study.

CHAPTER TWO: LITERATURE REVIEW

2.0 Overview

This chapter reviews literature that is in line with the problem of study. It is important to know that literature review have boundaries because it is practically impossible to review everything within the subject. The principal purpose of the literature review is to determine the educational and research area of which is relevant to the topic of the study. Furthermore, the literature review helps to locate and synthesize completed research reports, articles, books, and other materials on a selected research topic.

2.1 Functions of Libraries in Higher Institutions of Learning

Libraries are entrusted with the objectives of selection, acquisition, organization, storage, and dissemination of data to their patrons and this needs financial resources. (Matthew, 2004). The major function of higher learning institution libraries is to support their parent organization in achieving their objectives, just like the name suggest libraries are involved in providing support for research and academic activities in universities and colleges. This also includes the content, acquisition, technical services, providing institutional repositories, inter-library loans, and document delivery services (Matthew, 2004).

Chiemeke (2007) states that the first function of a library is to compile information or knowledge. Libraries are traditionally organized by functional departments, cataloguing, acquisitions, periodicals, and so forth to have it easy for accessibility of data. Chiemeke (2007) argues that the utilization of computers has also helped significantly within the functioning of libraries as they provide a particularly flexible way of sorting factual data, indexes, and catalogue entries. They provide hopes of reconciling the requirements of users and administrators, and of lightening necessary administrative operations like circulation and acquisition systems.

The other functions of an educational library are to supply a quiet reading environment for learners and lecturers and also the host community of the institution. Another function is to market research and supply research materials like bibliographies, abstracts. Libraries are also involved in marketing learning amongst students and lecturers by providing circular and reference materials like dictionaries, encyclopedias, manuals, atlases, gazetteers, monographs and books. They are also responsible in creating awareness of latest developments in science and technologies in the fields of learning to the university community. According to Moyo (2004), an honest library must provide

instruction on general resources to assist undergraduates and graduate students on how to find and using the specialized resources in their discipline.

According to Singh (2007), library collections constitute the bedrock for services provided to the community and function as important assets to the library. Therefore, securing and protecting library collections can help libraries provide an efficient service in response to the knowledge needs of the university community. The term collection security means there's a need for libraries to supply, maintain, and secure their collection to make sure longevity, accessibility, and effective provision of services to users. For libraries to realize this noble objective, it essential to have an efficient strategy to assess the degree of collection security, threats they are exposed to and establish a suitable level of collection security implementation to supply quality services (Campbell, 2006).

Chiemeke (2007), states that the majority of the universities have started paying greater attention to research by developing appropriate policies, making funds and facilities available for research, and inspiring their staff and students to try and do research. In many postgraduate programmes at universities, students are required to conduct a research project and submit a report as a pre-requisite for completing their degree. Faculty members also are needed to carry out research themselves, have more postgraduate students, and assessed through the outputs of their research. This has led to researchers making some demands to access information and on the standard of data provided (Singh & 2007).

The library's role is to promote scholarly publishing in their mother institutions may not be overemphasized since the state of scholarly publishing in any institution is claimed to be reflective of the speed of data generation and research output (Campbell, 2006). Taking cognizance of this, the University librarians are required to actively participate and sometimes create the acceptable forum for workers of the institution to urge them to be more involved in disseminating the result of their research through scholarly publishing (Campbell,2006).

2.2 The Necessity for a Library Security System

Educational libraries aim to provide information resources in both print and non-print formats. Balancing access and security in libraries may be a difficult thing to do but a necessary task. According to Dawe (2017) library materials are quite expensive to secure and preserve. These resources are very difficult to replace them once they disappear.

Many studies have described how crimes and security threat incidences can affect the supply of library services to users. Spagnoletti and Resca (2008) identified several incidents like theft of physical materials, theft or mutilation of print materials. The other types of threats include non-return of materials by borrowers and theft of library equipment, verbal and physical abuse against staff and users, and vandalism against library buildings and equipment, all these may directly or indirectly affect the supply of library services (Kumbhar & Veer, 2016). The other problems identified were underlining and highlighting text in library books, removing or tearing pages from books and book margins, thereby making it unusable to users.

Schmidts and Lian (2009) argues that it is necessary to ensure that theft, mutilation and vandalism are prevented because resources cannot be found in the library as they are expensive to replace. Therefore, security measures are necessary for preventing theft, mutilation and vandalism of library materials.

Simui (2004), argues that libraries of higher institutions of learning are battling with diminishing funds for the acquisition of library resources. The cost of books and other materials continues to go up, forcing many libraries to scale back or completely cancel Subscription (Simui & Kanyengo, 2001). Consistent with the University of Zambia (UNZA) annual report (2005), the University of Zambia Library is not excused from the challenges to do with funds to acquire periodicals and other information resources Simui (2004), echoed these concerns. The financial difficulties faced by academic libraries may render their role in institutions of upper learning irrelevant, as in most cases, they are failing to meet the knowledge needs of both the staff and researchers in their respective fields. Although the financial difficulties are directly faced by libraries, the impact trickles to patrons who happen to be lecturers and students in general hence, affecting the standard of learning and research output produced in academic institutions.

In this sense, higher institutions of learning must adopt security measures to stop the theft of library resources in academic libraries in Zambia. Security is a crucial and sophisticated challenge in contemporary societies. Not only do individuals require security and safety of their lives and properties, but also, organizations like libraries. In medicine, it's said prevention is better than cure, and also in libraries, good preventive measures particularly of storage and security should be adopted to stop damages and missing of data resources (Isebe, 2014). Since academic libraries face a variety of security

challenges with their collections (both print and electronic). It is imperative to secure and protect the collections as this can help libraries provide an efficient service in response to the knowledge needs of the users.

2.3 Types of Information Security Threats.

An essential step in security planning is to know what the organisation must protect before it plans relevant security measures to defend against those threats. That needs an awareness of the possible threats, vulnerabilities, and security issues confronting an organisation's employees, library users, data, computer systems, networks, and other library materials. Generally, security threats simply mean any security incidents which will directly or indirectly cause system vulnerabilities (Ogbonyomi, 2011). Threats become more specific when discussed within the context of vulnerabilities and attacks (Slade, 2006). The term vulnerability refers to weaknesses with the library system, human beings that expose a computer or user to exploit or a threat (Ogbonyomi, 2011). Vulnerabilities are often located in hardware, software, infrastructure, and processes (Zimerman, 2010). A threat itself cannot harm a system, but a successful attack does. An attack is an act that tries to bypass security controls and is also referred to as a realisation of a threat (Slade, 2006). Information system threat, for example, refers to a danger posed by an information system vulnerability that may cause undesirable consequences that may cause problems (Soomro, Shah & Ahmed, 2016).

Soomro, Shah and Ahmed (2016) surveyed the perception of management information system (MIS) executives regarding the safety threats in microcomputer, mainframe, and network environments. They developed an inventory of twelve security threats and empirically examined them. The results indicated that natural disasters, employee accidental actions such as entry of bad data and destruction of data, inadequate control over media, and unauthorized access to the accounting information system by hackers had been ranked among the highest security threats. Gautam,Behera and Singh (2011) replicated Soomro, Shah & Ahmed's study to get the present status of the safety issue in practice among data system auditors. The study established that employees enter bad data accidentally, the destruction of information, and the introduction of computer viruses were considered to be the three top threats in a microcomputer environment. In contrast, technological advances grow faster than control practice were said to be the foremost important threats in the network computer environment.

Fox et al (2011), identified different sorts of threats including human errors, system failures, natural disasters, and malicious acts. Yeh and Chang (2007), has categorised the threat resource for the (CMS) information systems into four main groups including such as environmental or physical threats, human threats, natural threats, and technical threats. Supported by this occurrence and significance within the current CMS environment, they also have divided the threats affecting major applications and other systems into human and technical threats. Whereas, the overall support systems are subject to environmental or physical, human, natural, and technical threats. Threats that are likely to affect the system are confidentiality, integrity, and availability. Carelessness, user abuse, theft, sabotage, vandalism or physical intrusions are identified to be the major human threats which may jeopardize confidentiality, integrity, and availability of information system. Whereas, the main technical threats to information systems' confidentiality, integrity, and availability include technical intrusion, unauthorised access to system resources, insertion of malicious code, database modification, system corruption, system errors, installation errors, and misrepresentation of identity.

2.3.1 Computer-based Information System Threats

With the introduction of Library Computer-based Information Systems by 1990, technology in libraries was seen as revolutionizing the concept of rapid and accurate information services (Slade, 2006). Currently, computer-based information systems are successfully introduced in many libraries and resource centres. With the inception of technology in libraries, terms like information technology, library automation and information communications technology computer-based information systems became common within the library world. Computers, telecommunications, and microelectronics are utilised in libraries for obtaining, storing, and transferring information.

Al-Suqri and Afzal (2007) noted that the power of a computer is to execute library functions quickly, accurately, and systematically makes it the most useful equipment. This is often because of the timely availability of data plays a fundamental role in the development of any organisation within the country. Therefore, computerised services in libraries such as housekeeping routines, information storage, retrieval, and networking become key to the delivery of efficient and effective services.

According to Ashenden (2008) there are various factors why libraries need information systems. Firstly, the explosive growth of the internet and its demands for connectivity requires extra external connections which have led to the creation of an outsized number of remote users (Kuzma, 2010). These users include employees who need remotely accessed to direct network connections to the remote office. Therefore, more libraries utilise information systems to help them in providing digitally delivered services and collections to local and remote patrons. Secondly, managing a library as an information centre requires a system that may process all sorts of information materials to supply the proper and accurate information to the proper patron at the proper time. Rathinasabapathy & Rajendran (2015), indicates that the library uses information and communication technology (ICT) in several ways. These include managing the library administration, processing of library materials, developing and accessing online resources, developing and accessing offline resources, and also to provide service to patrons.

However, the increased connectivity of the information system to the global village via the internet has changed the risks associated especially once they are connected without proper security measures. Yeh and Chang (2007) observed that threat related to the internet varies among libraries depending to the requirements of the organisation for information availability, confidentiality, and integrity. As an example, libraries should worry about issues associated with reliability, durability, and accessibility once they are relying heavily on digital content, partnering to distance education, creating in-house databases, and addressing technical challenges (Sundt, 2006). As highlighted by Zimerman (2010), the key components of a security plan contain well-managed access to services that protect online resources and user privacy while enabling simple use. This is often because information systems and networks are often inherently insecure since they are made with functionality not security as its primary goal (Hagen, Albrechtsen & Hovden, 2008).

Eisenberg & Lawthers (2008) utilised an Internet survey to review the various important levels of security control and sub-security controls in universities. Derived from the analysed responses from 159 data system administrators in IT centres of universities around the world. The study showed that authentication was the leading important security control in small and medium-sized organizations. However, confidentiality or integrity was viewed to be one of the most important security control in large size organisations. The results revealed that human issue was the last important security control in most of the organizations no matter the size. This study also revealed

that the importance of management support increases parallel with the dimensions of an organization. When compared, security awareness training was rated important only to large size organizations but small organisations viewed encryption technology as extremely important.

Clusif (2008), conducted an in-depth evaluation of Internet users' perception of computer threats and risks in France. The findings revealed that the dominant fears among Internet users were viral infections (86%), spyware (80%), intrusion (71%), spam (67%), phishing (67%), fraud (65%), hacking (54%) and equipment breakdown (46%). Zimerman (2010) conducted a study using questionnaires to know how organizations address their IT risks and to look at evaluations of IT risks performed by internal auditors in their organizations. The results of the study revealed that internal auditors focus totally on traditional IT risks and controls, like IT asset safeguarding, application processing, and data integrity, privacy, and security.

Abu-Musa (2010), conducted an empirical survey to research the many perceived computerized information system security threats in Saudi libraries. Four hundred questionnaires were randomly distributed to libraries of higher education institutions. The respondents were asked to point the frequency of occurrence of every security threat supported by five available choices (less than once a year, once a year to monthly, once a month to weekly, once every week to daily and quite once each day or more frequently). The results revealed that intentional and accidental entry of bad data, sharing of passwords, accidental destruction of information by employees, the introduction of computer viruses to Computer-based information system**,** and destruction of output, unauthorized access and directing prints and distributed information to unauthorized users are the most significant perceived security threats to organizations.

Farahmand et al. (2005), designed a comprehensive model for threat classification and control measures to a network system from three points of view, namely the threat agent, threat technique, and security measure. The researchers conducted case studies and interviewed six information system experts handling security issues. They identified threats to the information system of organizations like theft of proprietary or disclosure of data, virus or worm attacks, and denial of service attacks. Similarly, Baskerville (2005), also stated and believed that intentional security threats like hacking, computer viruses, and computer theft are getting to be more severe problems than other security

vulnerabilities. Olayemi (2005,) categorized threats to computer and network security into four groups such as physical threats, unauthorized access, accidental error, and malicious misuse.

Kimwele, Mwangi, and Kimani (2005) reported that 76.2% of respondents had suffered information system security threats in Kenyan libraries. The threats experienced by them included, user accidentally deleted files or changed computer configuration, deliberate attack in the form of hacking or disgruntled staff gained access, deleting or stealing data, software application misplaced causing re-installation delay, disk drive crashed causing loss of information and business disruption, copy failure such system restore failure because of corrupt or inadequate backups, data theft such as espionage which resulted in data loss and possible legal exposure, site disaster like fire or flood causing damage to systems and business disruption, infringement of copyright, for example, staff loading pirated software, and passing on confidential information. Unisys (2007), provided insights on the safety index among the Malaysian libraries of education institutions of higher learning towards different types of security issues. The study revealed that respondents were very or extremely concerned about computer security, viruses, and unsolicited emails. The survey also found that many respondents were very or extremely concerned about unauthorised access to or misuse of their personal information.

As numbers and different kinds of information system threats are constantly increasing, it has become impossible to present an entire list of threats. It may not be possible to cover all of them within the current library perspectives. Therefore, according to the relevant literature above the researcher will try to assess the present information system security threats in libraries and present a possible category of the overall information system security threats in the library settings.

2.3.2 Hardware Threats

Computer hardware forms a physical component in a data system and is additionally susceptible to security attacks. Kraemer, Carayon and Clem (2009) revealed several factors that jeopardise hardware security like natural disasters such as earthquakes, fires, floods, and thunder strokes, changes in temperature or humidity, accidents, stealing and vandalism, malicious intrusion and destruction, defects of the hardware itself, software or errors generated from routers or firewalls; and faults within the manufacture of the

equipment. Other issues are may do with air-conditioning failure, and loss of essential services like telecommunications or power.

Other hardware security threats, include electromagnetic interference, failure of communication systems and services, hardware breakdown, installation of unauthorised hardware, maintenance errors, physical sabotage or intentional destruction of computing equipment, theft of ICT hardware equipment.Yeh and Chang (2007) state that hardware infected with malware, computer viruses, worms, and Trojan horses may suffer some kind of damage like making it difficult to reboot the computer, repeated error messages, hardware malfunctions and this can lower the computing speed.

Computer hardware security measure, this equipment should be secured from any threats including thefts, power failures, equipment incompatibilities, damage and make sure the availability, confidentiality, and integrity of information within a library Yeh and Chang (2007). The measure of the present threat can be done through the use of loop television (CCTV), visual camera, magnetic detection system, and electronic anti-theft system at strategic places (Powell & Gillet, 2007). Besides that, the utilisation of locks, security cables, locked cable trays, metal cages, or anchoring devices is advisable for the shielding hardware equipment. Telephone lines are often cut or lost and electricity failure might happen, therefore a corporation should find alternative telephone lines as alternative communication lines and generators as backup power sources (Powell & Gillet, 2007). Besides that, physical damage to storage media like hard disks can always happen and might cause some data loss. Consequently, data recovery techniques like remote mirroring or file mirroring are often employed to save lots of important data. These remote mirror and replica feature is a hardware solution that permits the mirroring of knowledge from the local site to a second storage unit at another site or the remote site (Yeh & Chang, 2007).

Rajendran and Rathinasabapathy (2007) examined the effectiveness of electronic security systems at the biggest library of the University of Kentucky. They conducted a multi-phased project to find out if there was reduction of book loss after the installation of the security system. It had been found that after installing an electronic security system, book loss rates decreased. However, Greenwood and McKean argued that a manual checking system had some advantages to an electronic security system. Among the

explanations were patron deviousness in circumventing security systems and the surveillance system is quite expensive.

Merete, Albrechtsen and Hovden (2008), researched libraries that had electronic security systems. Twenty-four libraries of higher institutions of learning within the Mountains Plains region of the United States of America were surveyed to gauge the effectiveness of electronic security systems. The results reviewed that there have been two major kinds of academic libraries using electronic security systems. One group viewed detection systems as a tool to stop uncirculated items from leaving the library. Another group viewed the system as a way to catch and punish thieves. Olsen and Ostler concluded that those within the second group were more successful in protecting collections.

2.3.3 Software Security Threats

In terms of jeopardising software security, the threats are often divided into operating systems and related applications. Security threats accompany operating systems might include safety loopholes because of improper design and improper management. The software security threats that are related to applications include stealing software from the web and the contamination with viruses (Zimerman, 2009). Computer software infected with malware, computer viruses, worms, and Trojan horses may suffer some kind of damage such as periodically automatic reboots, program crashes or malfunctions, repeated error messages, and poorer system performance or unusual behaviour. Other software security threats include corruption by the system or system failure, maintenance errors, cyber-terrorism, software piracy, and unauthorized access, unauthorized changes to software settings, adware, spyware, hacking, password sniffing, weak passwords, and abuse of computer access control. Zimerman (2009), stated that software attacks can range from careful alterations to less careful changes. It must be also indicated that for the discreet alterations, attacks are subtly imposed for the aim of compromising the system. In contrast, for the less careful changes, attacks are intended to the destruction of information or other important systems features.

Several software security threats would jeopardise software security as follows: abuse of computer by employees or patrons abusing their access controls rights and privileges for private reasons or to get more data than needed for his or her jobs, adware and spyware may be a sort of malware which will be installed on computers to gather information about users without their knowledge. Specifically, adware is

employed as a marketing tool to watch people's behaviour on the web, to work out which products they like most (Etsebeth, 2007). While the functions of spyware go beyond simple monitoring because it can change computer settings, leading to slow connection speeds and loss of Internet connection or functionality of other programmes, corruption by the system, system errors, or failure of system software.

Zimerman (2009), echoed that system failure occurs when the delivered service does not comply with the specifications. Whereas a mistake is defined by (Etsebeth, 2007), as that part of the system which is susceptible to cause subsequent failure, and a mistake affecting the service is a sign that a failure occurs or has occurred. When the system comprises of multiple components, errors can cause a component failure. Malicious software can be accidentally or intentionally installed on computers from portable drives, email accounts, and web browsing. Allowing these programs to run on workstations presents a serious challenge to the IT administrators as internet threats such as malicious code, Trojans and Spyware could make desktop vulnerable to leakage of important corporate information (Harris, 2008).

A password is also vulnerablne to sniffing or stealing every time it is sent across a network when users are using remote access to access computers, printers, databases, emails, or internet banking. The integrity, reliability, confidentiality, and availability of the information processed by programme or software could be threatened if errors are made during the programme or software development, maintenance or installation process (Powell & Gillet, 2007). For instance, Microsoft sometime back in 1990s released software that made systems vulnerable to security threats such as Hotmail, Microsoft Outlook, and Outlook Express software. Microsoft Outlook and Outlook Express software had a bug that could allow malicious code to run on a computer without the knowledge of the user and allow the hacker to use the user's access rights to reformat the disk drive, change data, or communicate with other external sites.

The use of pirated or unauthorized software on the library network is illegal and places the library in peril of action by the software supplier. Therefore, ensuring that the software on library computer systems is fully licensed is the responsibility of the IT personnel as libraries are found to be in noncompliance, the consequences can be quite expensive. Unauthorised changes to software settings or programme code can be used to commit fraud, destroy data, or compromise the integrity of a computer system (Hagen, Albrechtsen

& Hovden, 2008). This would involve manipulation of settings in the browser such as to delete history files, change security settings, or enable private browsing. To prevent users from accidentally changing the system settings, a clear separation of functions between software programming staff and operational IT staff who implement all authorized changes should be made clear, use of library Internet for illegal or illicit communications or activities such as porn surfing, e-mail harassment, and cyber-terrorism refers to unlawful attacks and threats of attack against computers, networks and the information stored on cyberspace can cause fear and violence against persons or property (Zimerman, 2010).

The software security measure, flaws, and risks related to the library software are more likely to be found when services such as library systems, OPACs, online databases, and resources are made accessible via the Internet. Eisenberg and Lawthers (2005) suggested the use of the following measures for protecting the software security: clean up software to erase files or settings left behind by a user, desktop security software at the application level and operating level to watch, restrict usage or disable certain features of the workstations, distribution agents to automate the method of putting in an application or updates to workstations on a network, menu replacement software to replace the standard windows desktop interfaces and provide control on timeouts, logging and browsing activities, rollback software to keep track and record of any changes made to the computers and allow the system to be restored to its original starting point from any chosen point in time, and timer software to regulate the quantity of your time a patron can use a workstation (Eisenberg & Lawthers, 2005).

On the other hand, Yeh and Chang (2007) listed the following countermeasures to secure the software; use of multi-user operating systems and application software to allow concurrent access by multiple users of a computer. The use of periodical automatic debugging to remove any defects from newly developed software or hardware components, use of systems recovery to rebuild and repair the computer systems after disaster or crash, and regularly analyse the user entrance logs. Knapp, Franklin, Marshall and Byrd (2009), encourages organizations to use ID management software to automate administrative tasks and the use of a single sign-on system as user authentication and authorization to access all computers and systems. Despite that, an organisation should also consider the use of anti-spyware software, spam filtering software, and anti-phishing solutions to prevent any spyware, spamming, and phishing attacks as well as the web filtering software to prevent access to inappropriate materials or sites. Therefore, the scope

of software security in libraries should encompass the above components from software security threats and assure the confidentiality, availability, and integrity of the library software (Knapp, Franklin, Marshall & Byrd, 2009).

The workstation security measure, as more library services are made available to their patrons' Internet-connected computers, there is a requirement to secure each computer from any security threat from the web also as threats from the users like viruses and worms, theft, and unauthorized access (Fox & Eisherbiny, 2011). Creating a secure public access workstation involves many discrete procedures and these steps are interdependent with other security measures like network security, server security, and user issues (Eisenberg & Lawthers, 2005).

Eisenberg and Lawthers (2005) suggest several considerations so as to make secure public access workstations in libraries such as installation of the special third party lockdown software to customize operating system installations. The use of operating system hardening which is the process of modifying and locking down a typical default installation of the system on a server or a workstation. Also computers operating systems and applications especially for antivirus should be maintained up to date with the newest patches and updates, especially for antivirus and secure the computer 's BIOS. The computer should installed with less operating system features, secure or configure applications like browsers and office productivity. There is need to educate and constantly remind staff about the necessity for security, install desktop security software and private firewall to limit user access to a desktop and computer's operating system. Also desktop, printing functions and lots of applications, install rollback software, which resets a public access computer to a previous state whenever the computer is rebooted. Installation of clean up software that automates the method of deleting temporary files and cookies, install distribution agent which may automate the method of deploying software to several computers directly and need user authentication prior access to workstations (Eisenberg & Lawthers, 2005) .

Fox and Eisherbiny (2011) also urge, organizations to implement comprehensive desktop security and controls such as the implementation of role-based access control, host-based intrusion detection system, centralised automated antivirus solution, patch and update management system, monitoring system, software metering, personal firewall, and enterprise backup solution that covers the desktops. These initiatives should be

proactive instead of reactive with the blend of preventive, detective, and corrective to mitigate risks because of misuse and inappropriate desktop computers.

2.3.4 Network Security Threats

Chen, Wei. and Delis (2008), listed the common network security threats in libraries such as cracking of passwords, damage to equipment or data when lightning strike, surges or inadequate power, internet-based attacks of internal network resources, local patron tampering workstation desktop and hardware settings, unauthorized access to workstation file systems, including installation of private software, unauthorised access to server file systems, tampering local network infrastructure including network devices, network wiring, defacement of library sites if hosted on a library-based web server, theft of equipment, and inadequate funding to work, maintain and replace network equipment. Other network security threats that would threaten the network security include the following: Denial of service attacks (DoS) prevents legitimate users from making use of a service and often it is very hard to stop. The DoS attack may typically cause service interrupt and bonafide users losing confidence in the service or organization. Spying or sniffing take places when an attacker uses software to monitors or listens to all or any traffic activities and interprets all unprotected data like username-password combinations, confidential emails, and Master Card numbers.

Phishing software poses a significant risk to the network because it may often be utilized to capture sensitive network passwords and permit an attacker to try and do anything on the network (Farahmand et. al., 2005). Internet Protocol (IP) spoofing attacks occur when a hacker steals an authorized IP address, which may be a unique address for a node on a communication network. Typically, it's done by determining the IP address of a computer and waiting until the computer is not in use, then using the temporarily inactive IP address (Farahmand, et. al., 2005). The term Trojan horse simply means a program that performs the desired task but also includes unexpected functionality, accidental directing or re-routing of messages to a different person can cause a loss of confidentiality and integrity if these messages do not get protected and allowing authorized changes to be made before delivery to the first addressee, password attacks exist when hackers find a user who has system privileges with a simple password to realise unauthorized access to the system (Engebretson, 2011).

Session hijacking occurs when a hacker taps into a connection between a client and a server, then simulates the connection by using its Internet Protocol (IP) address. Farahmand et al, (2005) states that probes and scans ask unusual attempts to realise access or discover information about remote computers. Sometimes probes are followed by a more serious security event, but this often because of the results of curiosity or confusion. Whereas, scans such as port scan are often a prelude to a more directed attack on systems that the intruder has found to be vulnerable. Transmission errors may occur because of the failure of any of the network components that are used for the transmission of information. These errors can destroy the integrity and reliability of knowledge and may cause a loss of availability, while website defacement is an attack usually initiated by a system cracker who breaks into an internet server and changes the visual appearance of the web site. Penetration and hacking of internet sites are increasing because of the expansion of virtual private networks and online business, (Engebretson, 2015).

The network security measures and good security systems protect the network according to its purpose and this secure it from adware, spyware, or network intruders (Eisenberg & Lawthers, 2005). The network security for a library would be required to make full access of its bibliographic database to legitimate users on the internet and within the library also disallow access from unauthorized users. Eisenberg and Lawthers (2005) suggest for libraries to use firewalls as means to guard their internal network against attackers from the internt or outsiders also as providing for content filtering, web caching, and virus protection to the libraries' internal networks. Libraries are urged to think about the utilization of authentication, anti-virus software, desktop security software and separate cablings for every network or virtual LAN switches to physically separating public and staff local area networks (LANs), to guard the interior library networks security threats by internal patrons or staff. Besides these, libraries should also consider the utilization of firewall with virtual private network (VPN) capabilities to guard remote access connections especially for wireless network connectivity (Eisenberg & Lawthers, 2005).

The server security measure, servers play an important role in providing access to key library services like online databases, catalogues, and circulation systems to internal and remote patrons (Ridley, 2006). The supply, confidentiality, and integrity of the library server may often be assured via the proper implementation of specific countermeasures because it becomes accessible to those within and out of doors of the library. Therefore, libraries are required to take steps to secure e-mail and web server applications from any

intrusion and application failure because of viruses, hackers, and natural disasters. Kruger (2013) identified several technological security measures so as to guard servers at many various levels such as installation of firewall to guard servers from intrusion, hardened the server operating systems and also the server applications to guard from vulnerabilities, employ authentication to make sure that only authorised and valid users can access the system, installation of anti-virus software and keep anti-virus definition files up-to-date, provide physical security for the server like to put servers within a secure location as an example place it where there is a lockable cage , a locked room with environmental controls, review server logs periodically by employing a log file monitor utility which monitors log files for signs of intrusion or security violations, protect the filing system by restricting access to the directory structure using file or directory permissions, make regular backups for information , installation of software, hardware specifications and installation of passwords. Ridley (2006) noted that backup media and documentation should be placed at an offsite location, implement fault tolerance as a backup system if one system like a tough drive or the computer itself fails, install intrusion detection software, and host auditing software to monitor for signs of intrusion or changes on files and directories of computers or servers.

2.3.5 Data Security Threats

Data security simply means the practice of protecting and ensuring the privacy of individual or corporate data that resides in databases, network servers, or personal computers from corruption and unauthorized access (Hadow, 2009). Hadow (2009) considers threats to data constitutes destruction of data and resources, corruption or modification of information, theft, removal or loss of data and other resources, disclosure of information, and interruption of services. Other threats to data security may include data diddling or changing of information before or during input into a computer system, data loss because of wrong procedures of updating, storage or backup, data manipulation, delay in updating or dissemination, destruction through a natural disaster, exposure of patrons sensitive data through web attack. Other threats include impersonation or social engineering, loss of patron data or privacy ideas, and malware and malicious code like computer virus, worm, logic/time bombs, and trapdoor, masquerading of user identity, password attacks, sniffing, stealing, phishing or pharming, theft of proprietary data, unauthorized access, unauthorised data copying, unauthorized transfer of data, and accidental disclosure, modifications or alteration of knowledge. Malware refers to

computer viruses, worms, Trojans, and other computer viruses designed to wreck data by infecting open files and program of libraries on an operating system, deleting data and files within the hard drives, steal information, and send it to 3rd parties for illegitimate reasons (Hadow, 2009).

Since library stores, processes and provides access to vast amounts of knowledge like the patron records, personnel data, MARC records, and circulation data, and others, there is a need to have a sound data management system to assure the safety of its data against accidental loss, unauthorized modifications, and access by taking appropriate measures. Eisenberg and Lawthers (2005), suggested that the IT department should block all the physical ports like the Universal Serial Bus (USB) ports to stop information theft or data loss within the property right. Yeh and Chang (2007), listed seven countermeasures for shielding the information including the use of data backup, authentication for data access controls, authorization for user access rights, enforced path, event logging, and procedures for the management of removable media, information handling, and disposal of media.

The IBM Security Framework provides organizations with a baseline to assess their security posture holistically that addresses technical, behavioural, and managerial issues associated with information system security (Buecker et al., 2010). The model consists of six domains which include people and identity cover aspects on the way to assure that the authorised people have access to the assets at the proper time, data and knowledge cover aspects on the way to protect critical data in transit or at rest across the organisation, application and process cover aspects on the way to ensure application and business services security, network, server and endpoint. The IT infrastructure, cover aspects on the way to stay before emerging threats across IT system components, and physical infrastructure cover aspects on the way to leverage the potential for digital controls to secure events, people or things.

2.3.6 Physical Facilities and Environmental Threats

The most common problem of physical threats that has got to be factored into a security program includes natural disaster and theft (Ayoung, Boatbil & Sanbil, 2014). It was reported that the connection between physical threats and virtual threats is most apparent as both physical infrastructure and systems are needed to provide access point to the virtual world (Vacca, 2009). Vacca (2009), listed the common sorts of physical threats that include fire and smoke, water rising or falling, earthquakes, landslides or volcanoes,

storms lightning, sabotage or vandalism, explosion or destruction, building collapse, toxic materials, utility loss (power, heating, cooling, air), equipment failure, and Personnel loss, strikes, illness, access or transport. Perhaps the common prevalent threat is that of the natural calamity caused by natural and man-made environmental problems. Computing equipment, physical infrastructure assets, and data are often destroyed through fire, floods, electricity spikes, and power outages. Besides that, chemical, radiological, and biological hazards also can cause damage to equipment both from intentional attack or accidental discharge in the data system environment (Vacca, 2009).

Intrusion or authorised access into the library building is seen as another aspect that may cause theft of valuable materials. For example, stolen computing and network equipment are often resold on the black marketplace for less than their value. Additionally, physical attacks also can occur at system consoles through available Ethernet ports and in network equipment or wiring closets rooms (Hariyanto & Siahaan, 2016). Physical facilities and environmental threats, the term physical and environmental security refer to measures taken to guard the library systems, buildings, and related supporting infrastructure or resources which include air-con, power supply, water system and lighting against physical damage related to fire, flood and physical intrusion (Maidabino, 2011). The use of security personnel to undertake patrol within the library and to enforce appropriate library access at the major lobby has become increasingly common. However, they ought to not necessarily have access rights to information systems, sensitive output and secure all areas during quiet hours to stop the abuse of privilege.

According to Mansfield (2009), other uses of physical security systems in libraries include inspection of luggage and other belongings of library users while entering and leaving the library by security or library staff, visual inspection by library staff through floor walks to beat the unethical practices, and also the protection of windows with locks, grills, guards, bars, screens and films, door protection, case protection, and dummy security devises to controlled access to the library buildings and library collections. Rathinasabapathy and Rajendran(2015) also suggests the utilization of electronic security systems to beat the safety threats within the library by using the subsequent tools like burglar protection, supply alarm notification to responsible authorities, Electromagnetic system to combat library material theft, surveillance cameras to watch the library entry control and site surveillance, and frequency identification (RFID) system for straight forward handling and security of the library collection. These electronic security systems are believed to be

effective in reducing the incidences of theft and unethical practices within the library premises at a reasonable cost for several libraries.

Carey (2008), examined the planning of entrances and exits in Australian libraries. Buildings designed with just one exit seemed to be more successful in preventing theft. This was because buildings with few exits were easier to monitor. The conclusion was that future library buildings should have just one main entrance and exit.

Another popular physical security measure in libraries is that of using an air conditioner Trapskin (2008). This is often because the computers and their peripherals often have specific environmental requirements. Failing to meet environmental conditions specified by the manufacturer may cause machine failure and disputes over maintenance. Eisenberg and Lawthers (2005), also encourages the utilization of lightning protectors, fireproof or extinguisher installations, air conditioner, and quakeproof installations to guard the information system against physical damage through natural disasters.

2.3.7 Human Related Threats

Prior literature consistently reports that human errors are regarded as the most highly ranked security threats (Amini, Vakilimofrad & Saberi, 2021). There are instances of poor security practices that put an organisation's information system security in danger caused by human errors such as poor passwords selection, piggybacking, shoulder surfing, dumpster diving, installing unauthorised hardware and software, social engineering, access by unauthorized users, lack of discipline or knowledge among library staff and patrons and with no data backups (Amini, Vakilimofrad & Saberi, 2021). Munir (2012), indicated that computer fraud by insiders is recognised as a severe problem that might be difficult to stop especially when it blends with legitimate transactions. Human errors including data entry errors or carelessness, though often not considered as threats but highly likely to occur. Griffiths and Krol (2009), revealed that erroneous actions by employees or users can threaten the integrity, availability, confidentiality, and reliability of the information. For example, incorrect set-up of security measures could end in loss of confidentiality, integrity, and availability of information, switching off computers when a mistake is displayed rather than correctly closing all current applications, deletion of files, inadequate back-ups, and processing of incorrect versions of data.

Employee misconduct, especially in a large corporation could also be a major and difficult problem to manage, as the use of perfect intrusion detection controls become irrelevant when trusted employees either accidentally or unknowingly do something they ought to not do. Griffiths and Krol (2009) reported that 80% of the safety compromises come about because of actions by insiders. The consequences of employees' misconduct include loss of productivity, loss of revenue, legal liabilities, and other workplace issues. Therefore, organizations need effective countermeasures like enforcing appropriate usage policies to minimize their losses and increase productivity. Similarly, (Kraemer**,** Carayon & Clem, 2009) highlighted the danger of sabotage against sensitive systems by internal employees as they know the systems so well. Their knowledge provides them opportunities in sabotaging the organisation's computer systems. The common sabotage includes, destroying hardware and infrastructure; changing data; entering erroneous data; deleting software, planting logic bombs, deleting data, and planting an epidemic**.** Although the number of incidents of staff sabotage is believed to be not as much as theft and fraud but the individual losses are often high. Despite reports and findings on the seriousness of human errors in threatening information systems, these threats are poorly recognised as an important element for information system security.

Organizational measures (Process and Human dimensions), often human factor receives less attention in information systems security practices. Huge amounts of cash and time should be invested in technical solutions. Technical solutions are necessary to deal with vulnerabilities like viruses and denial of service attacks. However, many samples of security issues associated with humans such as phishing and social engineering increasingly exist. Therefore, depending on advanced technologies alone cannot solve the safety problem as technologies are generally served as static barriers and may become ineffective in an environment where humans exist (Hu, Dinev, Hart & Cooke, 2012). Recent research has also recognized the requirements to know the impact of human and organizational factors also because of the technological factors on the effectiveness of information system security controls. This is often because prevention of the misuse of information system security by employees has direct business value including increased productivity, maximization of corporate assets, compliance with privacy regulations, protection from legal liabilities, preservation of network bandwidth and resources (Hu, Dinev, Hart & Cooke, 2012). Therefore, organizations should deploy comprehensive

countermeasures that include human and organizational security measures to defend against the misuse of their resources like surveillance cameras and security guards.

Chao (2005) developed an information security assessment model to find out the safety level of an information security system in education institutions around the world. The assessment model comprised of a two-layer structure such as the safety controls and the sub-security controls which are formed and support information security systems, standards, best practices, and information security assessment guides. The security controls include authentication, access control, confidentiality, integrity control, audit, incident handling or disaster discovery, management, and people issues. This model is employed to verify the varying important levels of security controls and sub-security controls among different types and different sizes of institutions and organizations. This model is contributing to the improvement of the security evaluation metric over extant methods and provides a possible baseline for the quality of the information system security metric (Chao, 2005).

Salaam and Onifade ((2009), discussed the kinds of patrons who can cause problems. This list included those with mental problems like the schizophrenic, the paranoid, and the alcoholic. She also noted criminal types like exhibitionists, voyeurs, and child molesters. Further, it is also considered that the other potentially disturbing patrons are the elderly, children, and angry people. Rajendran and Rathinasabapathy (2007), looked at mutilation and theft of books and their relationship to electronic security systems. She surveyed educational libraries in Nigeria to find out if mutilation rates go up after an electronic security system is installed. This was discovered to be true. Rajendran & Rathinasabapathy stated that patrons are more likely to mutilate a book or periodical to get what they want instead of chance setting off the electronic security system by taking the whole book or periodical. As typically just one security strip is placed in each item, this strategy is successful in defeating the electronic security system most of the time. Due to this, theft will go down but Rajendran and Rathinasabapathy (2007) concluded that mutilation rates will rise after an electronic security system is installed.

Gupta and Sharman (2008) studied library criminal activity by watching two criminological theoretical groupings. One grouping was psychological theories that targeting individual traits. Another grouping was sociological theories which examine how societies are structured and the way this structuring might cause crime. Both groups can explain library

crime but it's difficult to work out if one or both groups accurately explain library crime in line with **(**Gupta & Sharman, 2008). Shamsul et al (2012), carried an empirical study in Nigeria on how library personnel can influence library security. The scholars believed that untrained library staff was liable for many of the library security problems. Staff unacquainted properly with security techniques and policies make it easy for security problems to exist and that alienate patrons engaged inappropriate behavior. Shamsul et al concluded that library staff should attend extensive security training.

Basaka et al (2020), reported on a study done at the library of Abubakar Tafawa Balewa University in Nigeria on theft of library materials and how they addressed the matter. The study revealed significant incidences of students and staff theft. Student and staff residences were searched and a lot of library books were recovered. As a result of the study, the library of Abubakar Tafawa Balewa tightened security and introduced identification cards to users. Oyewusi and Oyeboade (2009), listed several measures for preventing theft from libraries by library employees which include restricting access to rare materials to those that are directly liable for them, making detailed inventories of library materials, insuring all valuable material, and verifying that each one of the employees is honest by instantly investigating any suspicious behaviour. Oyewusi and Oyeboade (2009), recommended several steps for libraries to enhance security such as instituting a general amnesty week to allow stolen books to be returned without penalty, severe penalties should be delivered to bear on offenders like expulsion for learners and dismissal for workers' members and faculty, library training programs should inform students how harmful the theft of materials is to the library.

2.3.8 Book Based Security Threats

Most of the published literature on library security issues focuses on specific kinds of security threats**.** Omoike and Alabi (2020), highlighted theft, mutilation, and vandalism in the University of Ibadan, Nigeria as threats to library collections and proposed that libraries should formulate well-planned security measures to guard their collections. Physical weaknesses were also identified in libraries in terms of unsecured windows, faulty emergency exits, poor policies and unstaffed computer rooms, lack of security plans, poor security at the exits, inadequate loans and renewal periods, lack of security manuals, and poor signs are some of the causes of security threats. Mansfield (2009), identified abuse of materials in UK libraries which include theft of print and non-print materials, non-return of borrowed items, physical and verbal abuse, and vandalism of library buildings and

properties. Ewing also reported an estimated collection lost which is between 1500 and 3000 books stolen annually.

According to Alao, Folorunso, and Saka (2007), the libraries of upper learning institutions do not always remain safe and secure places as violence and property crime can and do occur intrinsically they become subject to many security concerns. The potential problems in libraries include include vandalism, theft and mutilation of library materials which is an ancient problem. Further, Ameen and Haider (2007) argue that the looting of the Great Library in Alexandria by soldiers of the Prophet within the Seventh century was the earliest recorded example. Folorunso, and Saka (2007), states that theft and mutilation of library books were world problems and historical ones.

Libraries of higher institutions of learning are information hubs that provide an area for learners and staff to carry out their research and advance their knowledge. Ultimately the objectives of libraries are to accumulate academic materials, preserve them from deterioration and loss, and to ensure that these materials are readily available to library patrons. This is done in order to satisfy the requirements of users (Maidabino & Zainab, 2011). Collection insecurity implies the necessity for libraries to supply, maintain, and secure their collection to make sure longevity, accessibility, and effective provision of services to users. To realize this important objective, however, libraries need an efficient strategy to assess the degree of collection insecurity they are exposed to and establish a suitable level of collection security implementation (Isebe, 2014).

In most instances, the security of stock in libraries is not considered a serious issue until librarians conduct an audit of stock and realize that a big number of collections is missing. A survey conducted by Salam & Onifade, (2010) within the Department of Library and knowledge Science, Federal Polytechnic, and the results showed that the annual loss of library materials in some of the academic libraries in Anambra State in the 1990s occurred. Presently, it might be much higher because numerous libraries don't perform stocktaking (Salam & Onifade, 2010).

The rate at which materials disappear in university libraries may not be over-emphasized. Miku, Buraimo, and Olusanya (2012) submitted that scandalous behaviour like theft and mutilation, hiding library materials, refusal to return overdue borrowed materials, drinking and eating within the library, among others became a standard occurrence in the academic library. If this is often not checked, it will cause a serious drought of materials within

the library. This is in line with Oyesiku, Buraimo, and Olusanya (2012) who stated that libraries in the developing nations, including Nigeria, lack security measures which inspire users to perform such unethical act of removing information resources in illegal ways. Apart from this, library materials are not found in great quantity in some libraries. Furthermore, most libraries were lacking photocopying facilities for users to use just in case of need. In some cases, when available, a power cut supply doesn't give room for users to have copies of urgently needed materials. This among other tempts causes users to behave in such a destructive act (Salam & Onifade, 2010).

According to Momodu (2002), libraries of higher institutions of learning are faced with varying degrees of criminal behavior within the use of their resources, especially printed materials, and to some extent manpower. The extent of this problem occurs differently from one library to another depending on the size of the library and the measures put in place. In some cases, the dimension of the matter is so restricted that it seems non-existent. In some others, the proportions are so massive that it becomes a cause for serious concern. It was also observed that stealing of library materials has been a long time problem of libraries. It is therefore, necessary to look at the library security management in libraries of of higher institutions of learning in order to supply quality services for the users making use of the collections. Library crime in academic libraries may be a global problem.

Security of library books and non-book materials has been the topic of much investigation. However, things seem to not be getting better (Nielson, 2002). Destructive habits of some users like theft, mutilation, and hiding of data materials pose a serious problem to other users who are often prevented from having access to library collections. Emerging from these good practices, library staff also experience difficulties in providing quality services while library management runs into a financial mess of replacing lost or damaged collections. Akussah and Bentil (2010) stated that theft and mutilation of books and non-book materials may be a common phenomenon in Nigerian university libraries, and if not checked, it can create a significant threat to library collections and their preservation.

Maidabino (2010), reported a high rate of book theft, mutilation, and misplacing of books and other library materials in Nigerian academic libraries. They suggested some measures to scale back the issues, which include tightening of security at library entrances and exits, the expulsion of scholars involved in theft and mutilation, provision of multiple copies of books that are heavily used, reducing the charges for photocopying, and periodic

searching of learners hostels and staff offices. Abioye and Adeow (2013), state that a successful inventorying process can help to spot the missing items; however, this might be hooked into the dimensions of the library's collection. They proposed the utilization of interlibrary loan (ILL) data failure cases to spot materials missing from a library's collection instead. Interlibrary loan helps libraries to borrow books which they do not have from other libraries on behalf of their library users.

Purtell (2007), stressed that university libraries must make sure that access and storage areas for collections are arranged and monitored for quick and straightforward inspection. The rare and special library materials should be stored separately, with folders kept separately within the collection to be easily checked by the staff. Furthermore, effective and reliable procedures to access library collections must be created. Accessibility to library collections can be enhanced by proper control and supervision of the library environment, especially designated areas for library assets. University library management must make sure that access to any area within the library is clearly defined and controlled. Library staff and security guards must also enforce restrictions by challenging unauthorized users in a non-confrontational manner (Trapskin**,** 2008).

Henrich and Richard (2016) highlight the importance of considering the safety aspects of the physical and infrastructural perspective of library buildings and facilities to make sure collection security, hence implicating an element that must be included within the assessment instrument. Chinwendu (2019), reported on a study on theft and mutilation of library materials in academic libraries: The Case Study of Kano University of Science and Technology, Wudil, Kano State, Nigeria and it was found that the periodical mutilation state was only 2.33%. However, the speed was higher for university libraries and 62.5% of university libraries considered periodical mutilation to be an outsized threat to the library collection. In contrast, there was not even one seminar in the library to consider this as a problem.

Isebe (2014), studied why students steal and mutilate books and periodicals. Questionnaires were distributed to students at one of the biggest urban university libraries. The results revealed that pressure to achieve a high academic environment appeared to motivate most theft and mutilation of library materials. Salaam and Onifade (2010), studied student perceptions of theft and mutilation in Nimbe Adedipe library, University of Agriculture Abeokuta. It had been learned that several assumptions

about the causes of periodical and book mutilation were true like student dissatisfaction or unfamiliarity with library services may result in theft and mutilation, lack of information about material replacement costs and time factor is another problem, lack of worry for others often prevents students from refraining from damaging collections and few students even know that library theft and mutilation may be a serious crime.

Mansfield (2009), researched incidences of theft and book mutilation in thirteen Nigerian academic libraries and it was concluded that there was a high rate of theft and book mutilation in Nigerian academic libraries. Interestingly, Osayande, (2009) looked at academic security concerns in Nigerian academic libraries. He examined crimes at Ilorin University including book theft and book mutilation and the results indicated that there was a relationship between high rates of security problems and the growth of a university. He concluded that the rapid growth of a university and the size of a library collection increase security problems.

Oyesiku, Buraimo, and Olusanya (2012), investigated disruptive readers at Olabisi Onabanjo University Library and a case study method was used to find out on destructive behavior among users of the library. The results revealed that disruptive behavior may be a common phenomenon among users of libraries. The study also indicated that limited materials, selfish interest among users and lack of photocopying facilities aid stealing and unlawful removal of parts of books and other materials. Other factors include ignorance or lack of orientation, lack of discipline and library materials might not be easily located when needed, and strike actions among others make users carry overdue materials, high registration fees and loss of original card were the explanations for using fake borrower's card.

Holt (2007), concentrated his study on internal theft from a library. Not all theft is perpetuated by patrons**.** Some library employees take material from the library without properly circulating it. As library employees' have skills to defeat the safety system since they know how it operates, this is in line with (Holt, 2007), who concluded it is one of the toughest kinds of theft to stop. Patrons also can cause security problems by their behavior within the library, even if they do not mutilate or steal.

Libraries of institutions of higher learning do spend huge sums of money to purchase library resources in an environment of small budget and insufficient funding (Odaro, 2019). Therefore, there is need to secure library resources from threats such as theft, mutilation and vandalism.

Security issues in libraries of higher education institutions is not only found in developing countries, but a global one. According to Oluwasanmi (2007) the issue of theft to library resources has been in existence as early as the development of libraries. Libraries have been fighting this problem for a long time without overcoming it and they have still continued fighting these security challenges. So many attempts have been made to address library security threats such as mutilation, theft and vandalism of library resources using both physical and technological methods.

The identified security issues such as theft and mutilation, vandalism, damages, and over-borrowing or irresponsible borrowers, and purposeful displacing of the arrangement of materials, are a number of the most security issues (Nielson, 2002). The abuse and mismanagement of library materials contribute greatly to the physical degradation of collections which include mutilation, careless handling, excessive photocopying, miss-shelving, and flicking documents over. As a result of all the safety issues and challenges presented, it becomes important for the researcher to research security measures adopted to stop the theft of library resources in selected academic libraries in Zambia

2.3.9 Human Aspect Security

Another factor is that of the human aspect security, mostly today security challenges are associated with the human aspect. This involves creating the proper atmosphere for greater security awareness amongst library staff, users, and the university community at large. According to Adewuyi and Adekanye (2011**),** criminal incidences in libraries include violent attacks on library employees. Besides, Abioye and Rasaki (2013) observed that physical assault of library staff and verbal attacks, harassment are some of the issues that can cause serious threats to a library. It becomes therefore imperative for libraries to document and implement measures to curb these situations within the library. Academic libraries and librarians globally require serene environments and safety incidences to effectively perform their mandates. This could be eventually an ideal scenario, however, things in most academic libraries in Africa do not seem to be anywhere closer to be ideal.

In a study conducted by Raffensperger (2010), it had been indicated that libraries found in urban centers stand a high risk of crime than those found in rural areas. These crimes may range from property destruction to more violent crimes against users and staff. Raffensperger (2010), further indicates that risk assessment in libraries should therefore

be comprehensive enough to incorporate personal safety and security. Recently constructed academic libraries must put several measures to make sure that the security of occupants of the library is guaranteed. These measures may include adequate ventilation, enough lighting, and the plainness of the library building (Dowlin, 2004). Akor (2013), further stressed that the library environment should be secured for collections, patrons, and also library staff.

A study conducted in Sam Jonah Library in Ghana by Akor (2012), indicated that the first goal of each security system within the library should target library materials, patrons, and also library staff. Therefore, library management needs to have a secure environment for library staff because the library cannot survive without staff. The safety and security of staff however is seemingly relegated and without any consideration. Attention should be placed on the safety of the library staff, especially during extended library services where the library closes at 10 pm within the semester and 5 am during examinations.

2.4. Good Governance

Another factor covered by the literature is the importance of excellent governance. Shafack (2021) proposed a security plan that comprises the following components: a written security policy, the appointment of a security manager, a security survey conducted to assess current and projected requirements such as identifying preventive measures like the installation of a security system, ensuring a secure premise during and after working hours, ensuring collection security through regular inventory, proper storage area, marking collections to determine ownership and instituting a tracking system of lost and over-borrowed items, and managing, educating and training users and staff.

The Association of School and Research Libraries (2006) suggested some guidelines for the safety of rare books, manuscripts, and special collections. One of the suggested recommendations is about the establishment of a proper governance system by hiring library security officers who can do the planning and administer security programmes, prepare and spearhead written policies. Libraries also need to closely monitor the entrances and exits of special collection reading areas, making staff conscious of collection security problems, providing training in security measures, monitoring of library users within the stacks, reading and reference areas, keeping adequate accession records, and aiding access through proper cataloguing and finding aids. The importance of

excellent and supportive governance with clear policies and procedures to take care of a suitable level of collective security in libraries is therefore vital (Guel, 2007).

Ayoung, Boatbill, and Banbil (2014), conducted a study on how secured library collections are in Ghana? The findings of this study showed that 77.8% of employees from different libraries have been trained in library and information studies. However, 50% of staff surveyed indicated that they did not attended any type of training on security issues to familiarize themselves with current trends within the profession since they were employed. Shamsul et al (2012) checked out how library personnel can influence library security. They believed that untrained library staff was liable for many of the library security problems. Staff unacquainted properly with security techniques and policies make it easy for security problems to exist and alienate patrons' engaged inappropriate behaviour. They concluded that library staff should attend extensive security training.

2.5 Security Policies of Library Collections

In general, policies are formal and high-level-broad statements that describe the required actions the organization wants to accomplish and why (Doherty & Fulford, 2006). Specifically, a security policy is a set of rules and practices that inform and regulate users, staff, and managers on how an organization manages, protects, and distributes its key assets including people, hardware and software resources, and data. Doherty & Fulford (2006), states that security policy may be a high-level management document that informs all users about the goals and constraints on employing a system and states who can access which resources in what manner.

Information security policy is a key area that requires to be taken into consideration, the common kinds of information security policies that are acceptable are copy policy, confidentiality policy, data retention policy, and wireless device policy (Knapp et al, 2009). The existence of such policies would reflect the highest management commitment towards all ICT security aspects and play as a reference framework to all or any other ICT security sub-policies, standards, procedures, and countermeasures in an organization. Hedström, Kolkowska, Karlsson and Allen (2011), suggests that the IT security policies should be reflective of ICT usage. As an example, an IT security policy will not be needed if there is limited or no ICT usage in libraries, but an in-depth policy that addresses all issues about usage of ICT infrastructure is required with sophisticated ICT usage.

Ashenden (2008), also suggested that libraries must develop an acceptable policy for computer usage that specifies what applications users can run, what data they will store, what they can browse on the Internet, what sort of activity is strictly or forbidden and what consequences will result if the policy is violated. In libraries, the safety policy is probably going to possess some areas of overlap with the suitable use policy. A suitable use policy is usually focused on patron use of the library information system, whereas a security policy is developed as an administrative guide, which incorporates rules and guidelines for accessing and use of information systems (Ashenden, 2008). The safety policy is required within a library to supply continuity, consistency, and a basis for enforcing staff and patron conduct on using the library information system (Soomro, Shah & Ahmed, 2016).

Haniza (2009), also studied the extent of enforcement and effectiveness of information security policy from the users' perspective in Malaysia at a public university. This study involved three phases of knowledge collection: a preliminary study to explore the IT arrangement and organizational structural practices within the university, an interview with an IT-expert to know the establishment of the information system security within the university, and the survey questionnaire to measure the extent of users' perception on the institution's security policy. The study found that almost half the respondents perceived that they were aware, understood, and accepted the university's policy. The majority of them agreed that the university's policy is effective.

Hu Dinev Hart and Cooke (2012), observed the importance of having a shared culture of mutual understanding for the safety and security of library resources. This is all about making clear to library patrons and staff about the security and security policies and also the guidelines on library operations, especially those regarding food consumption within the library, theft, mutilation, and disruptive behavior, and knowledge technology or computer systems. Roper, Grau, and Fischer (2005), also emphasized policies regarding the training of staff to make an awareness culture. The security issues about people aspect in the library may include staff's unconcerned attitudes towards users' needs and ignorance about security issues. Library staff at times are assigned responsibilities to guard the accessibility, confidentiality, and integrity of library materials as often the source of collection security problems Hu Dinev Hart and Cooke (2012). The results showed that people aspect and security culture are factors that are important when assessing collection security in libraries.

Hu Dinev Hart and Cooke (2012), top management is taken into account as critically important in developing a policy that involves ongoing capital investment and requires long-term planning. Udoumoh and Okoro (2007), also acknowledged other reasons why top management is seen as important for the success of the development of the policy which includes providing adequate support for policy development, commitment to policy development, accepting responsibility for policy development quality, and being responsible for forming and appointing the committee for all functional units to offer their full co-operation. Azerikatoa, Christopher and Sadat (2014) conducted a survey of Polytechnic Libraries in Ghana and the survey showed that few libraries were prepared for daily security problems. The overwhelming number of libraries had no written security policy. The results revealed that a lot of libraries had no definition what so ever, written policy or otherwise. These scholars recommended that academic libraries must create written security documents to guide library staff. Despite the issues of security faced by academic libraries, many librarians feel they have been doing a superb job in preventing security problems.

Abioye and Rasaki (2013) submitted that because of insufficient funding to libraries in Africa, these libraries are exposed to crimes such as theft and vandalism of library resources. This can be explained by the very fact that, insufficient funding makes it difficult for libraries to implement stringent measures to secure the library's collection, users, and also library staff. However, Abioye and Rasaki (2013), observed that absolute security is unfeasible in any organization. He further suggested that since it is not possible to exterminated crimes, prevention must focus on operative security and legal boundaries. In suggesting measures to curb crimes within the library, Anderson (2007), outlines among other security measures such as television cameras and enough security personnel to patrol all floors of the library should be implemented.

In Zambia, a study carried out by Kanyengo (2008) established that the University of Zambia and Copperbelt University libraries which are both funded by government, had been not receiving adequate funding up to date for their collections from early 1980s. The libraries have been building their collections mainly through donations and exchanges. Like any other library of higher learning institution the University of Zambia libraries have been striving to prevent their resources from crimes such as theft and vandalism (Shameenda, 2011). His study revealed that electronic security measures such surveillance cameras were put in place to protect library materials at the University of Zambia library.

It was further revealed that the University of Zambia libraries deployed some security guards to ensure that their materials are protected. The study showed that the use of security guards in these libraries was more prominent than any other security system.

The findings from the previous research have revealed that there are various categories of security controls deployed in various organizations. However, the extent of implementation of those security measures in many libraries was still lacking as they tend to focus totally on technical measures. Other studies have also found that the appliance of security measures in most libraries of higher institutions of learning was suffering from several factors such as the organization size and lack of funds for computer security. The study highlighted the necessity to assess the particular status or the extent of implementation of the various kinds of security controls in academic libraries and also because of the identification of the possible factors which could affect the extent of implementation of the safety measures in these libraries.

2.6 Gaps in the Literature Reviewed

It has been established that most of the literature reviewed in this chapter focused on theft and vandalism of library materials, the causes for the and mutilation. The studies conducted by Maidabino (2010); Mansfield (2009); Isebe (2014) and other scholars in Nigeria, United Kingdom and other countries throughout revealed that theft, mutilation and vandalism of library materials was common in libraries of higher institutions of learning. The results further revealed that pressure to achieve academic environment caused most theft and mutilation of library materials. It has been observed that prevention has not been discussed in depth especially for a library that lacks electronic system. The researcher also noted that discussion on solution to these problems have not been addressed satisfactorily because most literature concentrated on challenges which libraries are facing. The studies were helpful but could not satisfactorily address the problem of power outages especially in the night as this can cause loss of library resources.

The studies reviewed from Nigeria, Cameroon and other countries failed to address the holistic deployment of security measures such as the use of security guards and the electronic security system. For example**,** Shafack (2021); Rajendran and Rathinasabapathy (2007) and others did not answer the research question fully on security measures used for prevention of library materials from various security threats as the scholars only looked at the installation of cameras as a security measure. Library security measures must be comprehensive enough to

incorporate the use of different security systems such as security guards, generators and electronic security systems. However, most studies conducted only concentrated on the installation of security systems such as surveillance camera and alarm system. Looking at the insufficient coverage of the studies reviewed, there was need to carry out a study on security measures adopted by higher learning institutions libraries to protect their resources. It was also important to look at the challenges and benefits in Zambia, so the collected primary data is analysed. The collected and analysed data can help to answer the research questions precisely.

2.7 Summary of Chapter 2

The reviewed literature further showed that the main library's role is to providing access to information. The challenge to this is that libraries have been experiencing information security threats such as password sharing among library staff and unauthorized access to confidential information by hackers. Other issues are to do with deletion of data and lack of backup can lead to lose of data. Another threat is the introduction viruses to computer system which in the cause computer failure if the system is not updated regularly. It is a well-known fact that information storage, retrieval, and networking is key to the delivery of efficient and effective services to library users. Therefore, it is important that computers are regularly updated if patrons are to benefit from such services and this will also help the library to reduce on spending money to replace crushed computers. Another problem that was highlighted is to do with inadequate funding to work, maintain and replace network equipment.

Library resources are quite expensive to secure, preserve and they and they are difficult to replace them when they are lost with their inadequate resources. It for this reason that libraries thought it was wise to put in place some security measures to protect their precious resources from being abused. In the first place libraries deployed security guards in order to ensure that their materials were protected. These officers are place at the library entrance or exist to ensure that users are physically check as they enter and leave the library. Officers are also required to be patrolling in the library to prevent users from doing illegal activities. Generators have been also installed so that when power goes library services can normally.

It was further reviewed by literature that libraries have deployed electronic security systems to mitigate security problems which libraries are facing. Some of the measures include surveillance cameras to watch the library; frequency identification (RFID)

system for security of the library collection; 3M book detection system to prevent theft of print materials; smoke detectors to detect smoke in the library. These electronic security systems are believed to be effective in reducing theft and unethical practices in the library at a reasonable cost for many libraries.

However, these security measures have their own challenges as they cannot perform their functions when there is power outage. These devices are also expensive to purchase especially in developing countries where resources are very limited. Those that have managed to acquire them have difficulties to maintain them as they require to source expertise outside the country.

CHAPTER THREE: RESEARCH METHODOLOGY

3.0 Overview

This chapter covers the methods and procedures which was used to carry out the research. It covers the research design, study population, sampling procedures, data collection techniques, quality assurance, data analysis, and also methods of interpreting data.

3.1 Research Design

This study adopted qualitative research method and the approach used was exploratory research design and the strategy was descriptive survey research design. According to Green and thorogood (2009) qualitative research design is characterized by its aims. This simply means understanding of social life and the methods that generate words instead of numbers when analysing data. The research design wanted to answer questions like ‘’what’’, ‘’how’’ and ‘’why’’ of a phenomenon instead of how many or how much that are answered in quantitative methods of study. The research method was used because it was found to be appropriate for the study since the phenomena of security of library resources in libraries of higher learning institutions was the main focus of this study.

3.2 Population of the Study

A population is the collection of the elements which has some characteristic in common. Gay (2009) defines the study population as the larger group from which a given sample is chosen. In this study, the population of the study will be all libraries of high education institutions of learning in Zambia. The available statistics on the precise number of academic libraries in Zambia is not known, though the Higher Education Authority (HEA) estimated the total number to be approximately 302 registered higher institutions of learning spread across the country.

3.3 Sample Size and Sampling Procedure

A sample is the subset of the population and sampling is the process of selecting a small number of people for a study in such a way that the individuals chosen are going to be good key informants who can contribute greatly for the needed information to the research as they are considered to have an understanding of a given phenomenon (Gay et al, 2009). The sample size was 28 drawn from 15 librarie in this study were purposively selected. Samples in exploratory research are generally smaller and allowing an in-depth interview method. The researcher aimed to explain a specific situation in-depth and not generalize**.**

This study used a purposive sampling technique to pick a sample size of 15 academic libraries drawn from three provinces; namely; Lusaka, Central and Copperbelt provinces. This sample included libraries drawn from both public and private tertiary institutions of learning. The basic criteria for choosing these libraries is that the institutions should have fully established libraries manned by personnel with a minimum qualification of a Bachelor's Degree in Library Studies (BALIS).

3.4 Data Collection Instruments

To meet the research objects for this study, the researcher developed the following: interview schedules, observation method, policy documents, and secondary source of information. Ngulube (2007) observed that although no single method is ideal, if different methods give the exact answer, then the greater confidence may be placed within the validity of the conclusion.

The researcher sought a permission to carry out research. After being granted with permission, the researcher collected data as follows: For interviews, the researcher booked for appointments with the chosen participants. During the interviews, the researcher took notes and sound recording the interviews.

Observations were also conducted after the interview session as this could be used to clarify a number of the problems which were raised during the interview. Secondary sources of information were used and also Policy documents were identified during the interviews and more data was collected after the interview sessions through downloads from the universities of higher institutions of learning websites or were emailed by the respondents.

3.4.1 Interview Schedules

According to Chifwepa (2006), an interview may be referred to as a method of administering a questionnaire that involves face-to-face interaction with the subject. Gay (2009) argues that the interview method of data collection has the subsequent advantages: useful when participants might not be directly observed, participants can provide historical information, and allows researchers control over the line of questioning.

Chifwepa (2006) stated that interview guide is employed to expand the knowledge that was collected through a questionnaire. One of the drawbacks of using semi-structured interviews is that they depend upon the expertise of the interviewer. As an example, the power to consider questions during the interview and articulate them to the

interviewee might not be as easy as one might expect. Unstructured and semi-structured questions are going to be prepared and will be used to elicit views and opinions from the participants. The interview schedule was prepared in line with the objectives of the study and also the research questions. The data collected will help to satisfy the study objectives. As a validity check, the researcher will use telephone interviews for clarification on issues that will not be clear during transcription or as to how to verify given information.

3.4.2 Observation

The unstructured observation method was used in this study to solicit information. This is a process that assist the researcher to know more about the elements under study by observing and participating in those activities Kawulich (2005). The aim was to understand the processes the elements in the context to get the needed information. The method was adopted as it was found to be appropriate for this study because it can give rich qualitative data. During observation process notes were written down to collect data, while conversations with participants continued. Documents with need information were also looked at to seek data.

3.4.3 Secondary Information Sources

Secondary information sources can be described as data that is neither collected directly by the user nor specifically for the user. This involves gathering data that has already been collected by somebody else. This is often the gathering and analysis of published material, and knowledge from internal sources (Kombo, 2006). Gay (2009), argues that using secondary sources of data is advantageous because researchers obtain the language and words of participants, often accessed at a time convenient to the researcher. Unconstructive source of data represents data which is meaningful therein participants have given attention to compiling it, as written evidence. It saves the researcher time and expense of transcribing. Secondary information sources that will be used include policies and strategic plans of the organizations and those to do with institutional libraries. These will explain security systems, preparedness, reaction, and recovery procedures for computer-based information systems and also the content coverage, persons responsible, and their responsibilities.

3.5 The Reliability and Validity of the Instruments

Before data collection, the interview schedules were tested to eliminate any ambiguities and mistakes. Gay et al, (2009), warned that regardless of how carefully one designed information collecting instrument there will be always a likelihood of error. Pre-testing allowed the researcher to spot items from both the interview schedule which did not

elicit the data needed and poor instructions or missing questions. The interview schedule was tested on one IT professional and three librarians within UNZA Library. These employees were conveniently selected to participate in the pilot study.

Kombo (2006) caution researchers against threats to validity and reliability, which may never be eliminated. Reliability is when there is consistency of a measure and validity is when there is accuracy of the measure. When the same results are consistently achieved by using the same methods, the measurement then can be considered reliable but if research has high validity, this means it produces results that correspond to characteristics and variations in the physical world. The author suggest that what is often done during design, data gathering, data analysis, and data reporting is to undertake and minimize the threats. With this regard, an assessment of the information hinges upon determining the reliability and validity of the research instruments used. Creswell (2009), defined validity as the degree to which a test measured, what is it alleged to measure. During this instance, questions were structured for interview schedules. This was achieved by ensuring that questions were associated with the matter under investigation.

Semi-structured interviews, instead of using the terms reliability and validity, Israel and Hay, 2006), prefer the terms credibility, dependability, conformability, and transferability when working with qualitative data. Therefore, instead of striving for validity, every effort were made to guard the credibility of the research findings. To make sure the interview data were credible, a member was used check participants. After the interviews and preliminary stage of data analysis are completed, the researcher synthesized the information from each participant. In qualitative research, reliability is represented by the dependability or consistency of the findings. The researcher made sure that the research process is consistent, logical, and documented. Dependability is going to be enhanced by the preparation of an interview guide and conducting a member check with the participants.

Confirmability refers to the objectivity of the study. This is concerned with the interpretations of data by the researcher accurately and properly describe the truth they set to portray. To reinforce confirmability, the researcher consulted his academic supervisors throughout the research process, continuously questioning the research findings and critically reviewing the information on an on-going basis. Finally, the small sample size affects the transferability (generalizability) of the research to a

bigger population. However, this is often to not suggest that the findings might not be useful to inform the research. When using qualitative research, transferability becomes the responsibility of the one doing the generalizing. The individual who is curious about the results to a special context or setting is liable for judging whether or not the transfer is acceptable (Israel & Hay, 2006).

3.6 Data Analysis

According to Oso and Onen (2005), data analysis deals with its organization, interpretation, and presentation. It is a complex process of selection, sharpening, sorting, focusing, discarding, and organizing to make sense out of the data, integrating it, drawing conclusions, and verifying it (Israel & Hay, 2006). Collected data was organized and ready for data analysis. This involved transcribing interviews, optically scanning the materials, typing field notes, sorting and arranging the information into different types according to the sources of data. The researcher read through the information to get a general sense of the knowledge and to reflect on its overall meaning.

Qualitative data that was collected through interviews, observation method and from the documents and was grouped according to themes, as themes and sub-themes emerged from the data. According to Oso and Onen (2005), this can help to facilitate browsing the research questions and interview responses and come up with common themes concerning each of the questions. The responses from interviews were put into categories according to the emerging themes. This allowed objectivity and important interpretation and this also helped to make decisions that were valid for proper conclusion and recommendations of the study.

The detailed analysis was done using a coding process which entails organizing the materials into chunks 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 a particular language of the participant (Creswell, 2009). In this case, numeric codes was used to categorize data according to the identified themes. The researcher analyzed the collected data using thematic analysis after organizing it into themes which were derived from the research objectives and the research questions. Narratives was used to report the findings and some data was presented in Tables.

3.7 Summary of Chapter 3

This chapter explains how the study was conducted, that is, what was done to gather data to answer the research questions. It states the data collection plan, and also specify the techniques which were used for data analysis. Its aim was, amongst other reasons, to assist other researchers to replicate the study if need be.

The approach used to this study was qualitative research design and the strategy was descriptive survey research design. This kind of approach was preferred because the subject is comparatively new. The sample size of the study comprised of 45 respondents which were drawn from 15 libraries of higher education institutions. These libraries were drawn from three provinces; namely; Lusaka, Central and Copperbelt provinces.

The interview schedule was prepared in line with the objectives of the study and also the research questions. The researcher developed the following instruments: interview schedules, secondary sources and observation checklist. Before data collection, interview schedules were test to ensure that miskes were eliminated. Detailed analysis was done using a coding process which entails organizing the material into chunks or segments of text before bringing meaning to information. The collected data was analyzed using thematic analysis after organizing it into themes that were derived from the research objectives and the research questions. Narratives was used to report the findings of the research. The major problem encountered was the unavailability of some respondents as they had other commitments. However, this problem was resolved by phoning those respondents who were not found.

CHAPTER FOUR: PRESENTATION OF FINDINGS

4.0 Overview

This chapter presents the research findings of the study which assessed the security systems in selected academic libraries of higher institutions of learning in Zambia. Interviews were carried out from twenty-eight (28) participants and collected data were thematically analyzed. The chapter is divided into the following sub-headings: demographic characteristics of respondents, the types of security problems being faced by academic libraries in Zambia, security measures libraries of higher education institutions put in place to mitigate against security problems libraries are facing and the effectiveness of the security systems used by academic libraries understudy, suggestions from respondents on how to overcome the challenges and summary of the findings. The study presents the findings on specific research objectives.

a) establish the types of security problems being faced by academic libraries in Zambia
b) establish security measures academic libraries have put in place to mitigate against security problems libraries are facing.
c) determine the effectiveness of the security systems used by academic libraries under Study.

4.1 Response Rate

Out of the total number of 45 respondents, 28 were interviewed as shown on table one below. The poor response rate was due to the busy schedule of respondents. The study targeted circulations librarians, System Librarians, and Chief/Deputy Librarians.

Table 1: Demographic Characteristics

Demographic characteristics		Frequency
Gender	Male	14
	Female	14
Age	31 - 40 years	20
	41 - 50 years	5
	Above 50 years	2
Academic qualification	Master's Degree	3
	Bachelor's Degree	14
	Diploma	7
	Certificate	4
Institutional affiliation of respondents	Universities	11
	Colleges	3
Position of Librarians	Acting Librarian	1
	Assistant Librarian	15
	Chief librarian	2
	Deputy librarian	2
	ICT Manager	3
	Library Assistant	4
	Sub librarian	1
Work experience	1 – 5 years	15
	6 – 10 years	3
	11 – 15 years	5
	16 – 20 years	3
	Above 21 years	2

4.2 Respondents that participated in the study

Among those who participated in the study were 14 male and 14 female. The age arrange from 31-40 years were 20, 41-50 years 5 and above 50 years 2. In terms of education master's degree were 3, bachelor's degree 14, diploma 7 and certificate were 4. In this study 11 universities and 3 colleges participated. The positions for participants included 1 acting librarian, 15 assistant librarian, 2 chief librarian, 2 deputy librarian, 3 ICT managers, 4 library assistants and 1 sub

librarian. With regard to work experience from 1-5 years were 15, 6-10 years 3, 11-15 years 5, 16-20 years 2 and above 21 years were 2.

4.3 Problems Faced Regarding Print Materials by Libraries of Higher Education Institutions in Zambia

This section provides the findings of the study on types of security problems being faced by libraries of higher education institutions in Zambia and the following were the results of the study:

4.3.1 Theft of Print Materials

The findings of the study shows that all the fifteen libraries under study experienced theft of library books, journals, and past examination papers by users. Respondents were further asked to indicate the type of books which were lost most. The most vulnerable materials were in the School of Law, Engineering, Medicine, and Education. Respondents were asked to state their opinions as to why libraries lost books in these fields most. The results indicated that materials from these fields were targeted because they were in high demand; selfish patrons; expensive; and difficult to find. Respondents further indicated that library users stole library materials most when the power went off, especially at night because security guards found it difficult to check for library materials as users were exiting the library. The study revealed that book theft was a major problem in most libraries. *"We usually experienced a loss of book, journals and past papers"* one *respondent observed."*

4.3.2 Mutilation of Print Materials

The study indicated that all the libraries experienced mutilation of library books, journals, and past papers by users. When respondents were further asked the type of books which were mutilated most. The results revealed that the majority of libraries had Educational and Social Science books mutilated most, while few libraries had their medicine books mutilated most. The study further indicated that three libraries had Law and Engineering books mutilated most. Respondents were asked as to why these books were mutilated most. Respondents indicated that libraries such books were mutilated most because they were in short supply on the market and expensive to buy when found. Respondents further indicated that such books were on demand. The results further indicated that these books were mutilated most because of the selfishness of readers as they wanted to pass alone. The study revealed that mutilated books tend to lose their usefulness which forces libraries to replace such materials. *"Students usually*

tore off pages of interest from the books and take the pages with them as they leave the library and sockets were removed" observed one respondent.

Table 2 below revealed that there were five common methods used by library users to steal library materials. The results revealed that all the fifteen institutions under study have lost their materials through patrons concealing books in their clothes as a sure way of smuggling books out of the library especially libraries that did not have a 3M security gate. The results further indicated that it was difficult to catch a thief when they hide books in their clothes especially when a library did not have a 3M security gate and CCTV cameras. Table 2 below shows that more than half of the libraries experienced where library users stole library books by evading or avoiding the security system so that when they were not checked as they smuggle library materials. This was another way of removing library materials illegally.

The study further indicated that library users would open the window and throw the books outside when windows did not have mesh wire. The study further revealed that few libraries had lost library materials through impersonation. This was where library users stole library books by using someone else's ID. The results revealed that library users would pretend that he/she was carrying his ID. The study also indicated that respondents from a few libraries revealed that patrons stole library materials by packing them in their bags. Respondents further indicated that it was for the reason that patrons were not allowed to enter the library with their bags.

Table 2: How users steal library materials

Rank	**Methods used by library users to steal materials**
1	Concealing books in clothes
2	Evading security checks
3	Throwing books through windows
4	Impersonation
5	Hiding books in bags

Different methods were used to steal materials from the library. These included concealing books in the clothes, evading checkpoints, hiding them in their bags. Some library users stole the identity cards of their fellow students and use them to borrow books out of the library with

an intention of not returning such materials. Library users also stole materials by pushing them through windows.

4.4 Challenges Encountered in Ensuring the Security of the Library Resources

This section discusses the challenges library management faced in ensuring the security of library resources. Respondents were asked to explain the challenges they encountered in ensuring the security of information resources in their libraries. The results of the study revealed the following:

4.4.1Inadequate Funding

The study revealed that more than half of the libraries surveyed were facing inadequate funding to purchase and maintain security systems and this was seen as the main challenge or hindrance experienced by libraries in ensuring security in the libraries. The results also indicated that respondents would wish to have the latest security systems in their libraries, but money had been always the major challenge. One respondent mentioned that: "*inadequate funds have hindered us from acquiring modern equipment to ensure maximum security in the library as the equipment has become very expensive.*

4.4.2 Loss of Information due to Change in Technology

Respondents from a lot of libraries indicated that their libraries experienced disaster when migrating from one technology to another and data was lost during this period because the two were not compatible. For example, the hard disk was used for data storage and this information was accessed using computers with a hard disk slot which is not the case with the latest computers as they have a provision for flash drives. It was this data from the hard disk that could not be accessed using modern computers which do not have hard disk slot. One respondent observed that*: "When a new technology is introduced there are always issues to do with records not being migrated to the new system and data is lost through this process of technology change is a threat to computer-based information system".*

4.4.3 Password Sharing among Library Staff

The study sought to find out whether libraries had experienced any sharing of passwords by library staff. The study revealed that six libraries experienced a problem where employees shared passwords for their computers causing a threat to computer-based information system (CBIS). The results showed that this was common at the issue desk where one password was given to some employees working at the issue circulation. The results also indicated that five libraries did not experienced that problem. The findings further revealed that casual employees

were given a password by their colleagues when given duties at the circulation desk or when working night shifts when those employed permanently were not available.

The results of the study further showed that library employees had been reported to have compromised the circulation system by issuing library materials to themselves and later discharge them from the system without physically returning the books. The study also revealed that at times staff were just putting a date due stamp on books that were not checked out the system so that they could pass at the checkpoint easily without a problem. The findings further indicated that the passwords given were supposed to be confidential and strictly used by an individual who was given the authority to access certain information or data. One respondent noted that: "*We are using a common password at the issue desk or circulation desk which almost everyone knows. Everybody comes here to work when on duty roster and this becomes a risk to other data because when I log in, I can access circulation, overdue fine and I might not be around throughout the whole day. Someone can clear a student with an overdue fine; check out books to steal using my account".*

4.4.4 Incompetent Staff

The findings revealed that respondents from a lot of libraries indicated that they were not competent to handle the security of the information systems, while respondents from few libraries indicated that they were trained and competent in information systems.

4.4.5 Inadequate or Absence of Policies Relating to Security Management of Information Systems

The study showed that half of the libraries surveyed did not have written policies and programs that focus on security management for the information system in the library. A few respondents from libraries that had policies were further asked if policies were accessible. The findings revealed that policies in these libraries were accessible. When the researcher request to have access to policy documents from these libraries, respondents were able to present the documents to the researcher. The policy documents contain information regarding the objectives or aims, how the information should be organized or who has the responsibility for what, and also the confidentiality of the information. Concerning whether the librarians were involved in developing the policies, the study revealed that library staff from three libraries were involved in developing the policies. The respondents were further asked the basis on which they were involved and what their contributions were. The study revealed that respondents were involved because they were in charge of ICT security and their contribution was on how best to protect computers and information. Respondents were further asked if the

policies or programmes were updated and if so by whom? The findings further revealed that the policies were updated by the librarians and ICT personnel. When asked if they were tested before approval and the study revealed that they test them before approval**.**

4.4.6 Poor Maintenance of ICT Infrastructure

Respondents were asked if computers were adequately maintained, serviced, and replaced damaged equipment. The results show that computers from six libraries were not adequately maintained, serviced, and replaced damaged equipment, while computers from nine libraries were adequately maintained, serviced, and replaced damaged equipment. The study discovered that there was poor maintenance, servicing, and replacement of damaged materials because of bureaucracy. One respondent argued that: *"The library poorly maintains, servicing and replace damaged because of bureaucracy involved"*.

Respondents were further asked whether their libraries cooperated with the ICT department in ensuring security for a computer-based information system (CBIS) in the library. The study revealed that respondents in most of the libraries cooperated with the ICT department in ensuring security for CBIS in the library, while few respondents indicated that there was no cooperation. Respondents were further asked the way libraries cooperated with the ICT department. The study revealed that the library management system was networked with the ICT department so that they could help to update the system when there was a problem and also help when the system was down. The study further indicated that the ICT department helped to install the antivirus software, training of staff, internet connectivity, and to provide maintenance to computer-based infrastructure.

4.4.7 Inadequate Security for Library Staff and Users

To establish the security problems which library staff and library users were facing, respondents were asked to state the problems they experienced. The results of the study revealed that library staff in more than half of the libraries did not have challenges, as they were provided with transport and also security guards, were available up to the time when libraries were closing late, while respondents from the minority of libraries indicated that they had a challenge because they were not provided with security guards in their libraries and also transport was not provided to them when working late, but instead they were given transport money. "*Library users were always coming to us to complain about their fighting over chairs, tables, and reading space*." One respondent observed that.

4.5 Physical or Manual Security Measures Academic Libraries have put in Place to Mitigate Against Security Problems

This section provides findings regarding types of security measures that were put in place to mitigate security problems libraries were facing. The results indicated seven different types of physical security measures that were used in libraries and they were presented in table 3 below ranked in descending order.

Table 3: Security measures put in place to mitigate against security problems

Ranking	Physical or manual security measures
1	Inscribing library materials
2	Cloakroom
3	Fire extinguishers
4	Books not returned
5	IDs
6	Security guards
7	Windows and door protection

4.5.1 Inscribing Library Materials

Table 3 above revealed that out of seven physical or manual security measures listed above, an ownership stamp was used by all the libraries' understudy. The researcher asked for permission to observe or physically check for the stamps in print materials and true to the responses from respondents libraries do inscribe their materials for security reasons. The results further indicated that less than half of the libraries stamped their print materials with ownership stamp on the title page, the middle page which is a secret page, and the last page, while respondents from few libraries indicated that they stamped their print materials on versal page, any page in the middle which is a secret page and any other page towards the end.'' *We ensure that the newly received materials are protected from theft putting ownership stamp on them."* Said one respondent. The results also showed that four libraries did not have selected pages but just stamped on any pages inside the material, while print materials in one library were stamped on the title page, index page, on the edges of pages if the book was big enough to be stamped and also on a specific secrete page number. The study revealed that secret page numbers could not be indicated because of security and ethical reasons. The results further revealed that accession

numbers, barcode numbers were also used and one library had serial numbers generated using the information management system.

When respondents were asked how effective was the ownership stamp that was put in place as a security measure on print materials. The study revealed that respondents from most of the libraries indicated that, ownership stamp was effective because security guards and library staff were able to identify library material from personal copies for library users. The study also indicated that the ownership stamp was effective because secret page numbers were used to quickly identify materials that library users did not know. The results further indicated that there were other security features that libraries used as measures to print materials, such as accession numbers, barcode numbers, and serial numbers generated using the information management system. The study showed that it was difficult for a thief to see all those security features and temper with them. One respondent mentioned that: '*Since library staff and security guards know the secret pages where the security feature are put it is to identify library materials at the exit when readers are leaving the library.''*

However, respondents from the a few libraries were of the view that the security measures were not effective because thieves were able to remove the pages which had security features when they identified them and went out of the library with library books without the security guards being able to identify library materials. One respondent observed that: *'We had a serious challenge to convince a student who tempered with ownership stamp and other security feature on a library book because all the pages which had features were removed, he also went ahead to remove other pages which he felt were not necessary so that we could easily give away"*

4.5.2 Cloakroom

In trying to establish the security measures that were put in place to protect users' belongings, respondents were asked to state the measures that they had put in place. The study indicated that all respondents from libraries under study had cloakrooms or locker/cabinet which was a designated area for safekeeping of users' bags. An observation was carried out in these libraries to find out if they had designated cloakrooms and the findings showed that only few libraries had designed cloakrooms. Some of the libraries are using lockers/ cabinets to secure user's belongings. The results further indicated that in some libraries when a user left the bag at the cloakroom the person was given a tag with a number representing that particular position where the bag was put or placed and when a user wants to get the bag from the cloakroom he/she was to present the tag to the officer manning the place and the bag was given to the owner. "*The establishment of the cloakroom at our library has helped to reduce theft of library materials.*

When users come in the library we ask them to leave their bags at the cloakroom". One respondent said that.

Consequently, when respondents were further asked whether they had received complaints from library users where they had lost their items from the cloakroom. The study revealed that a lot libraries received complaints where library users lost their items from the cloakroom. However, only a few libraries did not receive such complaints from library users.

Respondents were further asked to state the items which library users lost most at the cloakroom. The findings of the study revealed that most library users lost personal textbooks, notebooks, laptops, and bags. Respondents were further asked how frequently they received reports about stolen items and the response revealed that six libraries received complaints once in a while and four libraries did not receive any report. The findings further revealed that respondents from three libraries indicated once in a month, while two libraries received complaints once or twice in a semester. The results further showed that one library did not receive any report because the library was small and bags were kept in a cabinet/lockers next to the issue desk which made it easier to monitor. *"At times library users would come to us and complain about their lost items such as laptops, textbooks and bags. We suspect that users steal amongst themselves thought might incidences where outsiders come in to steal"*. Said one respondent.

The study further revealed that readers were not allowed to enter the library with water and food, patrons were asked to leave them at the cloakroom. Respondents indicated that water was not allowed because it could spill on books and stain them. The results showed that water also destroys books as it would make pages of books sticky to each other when drying them up and this made words to be not clear. The study further revealed that food particles attracted rodents or insects which could eat and stain books as they left their droppings.

The study revealed that a cloakroom was a place designed in a library where users were required to leave their belongings to avoid a situation where readers start putting library materials in their bags. The study further indicated that at this place there was always a need to have a security officer or library staff receiving and giving out bags to users so that theft was prevented. The study findings further indicated that readers used to pack library books in their bags and it was for this reason that readers were not allowed to go into the library with their bags. One respondent noted that: "*Bags could be used to carry water, food and even dangerous*

weapons that were not allowed in the library. We ensure that patrons leave their food and water so that it does not spill on books". Observed one respondent.

In trying to establish the effectiveness of the cloakroom that was put in place as a security measure to protect people's items. The study revealed that a lot of libraries indicated that the measure was quite effective because libraries rarely received complaints from library users having lost their items from the cloakroom or locker/cabinet where bags were kept. The results indicated that security officers or library staff who were in charge of the cloakroom did not allow library users to get bags on their own and this reduced theft**.** However, respondents from a lot of libraries indicated that the security system was not effective because library users had continued losing their items from the cloakroom.

4.5.3 Fire Extinguishers

The study sought to find out whether libraries had put in place fire extinguishers as a security measure to mitigate fire in academic libraries, respondents were asked. The findings in Table 3 above revealed that out of seven physical or manual security measures listed above, fire extinguishers were used by all the fifteen libraries under study. The observation method also proved that libraries installed fire extinguisher though in some libraries the gadgets had accumulated dust as if they are no longer cared for. When asked if fire extinguishers in their libraries were serviced. The results indicated that respondents from more than half of the libraries were of the view that fire extinguishers in their libraries were not serviced, while respondents from few libraries indicated that they were serviced.

Respondents were further asked if they knew how to use fire extinguishers, the results from most of the libraries indicated that they did not know how to use a fire extinguisher. This shows that most of the staff were not trained on how to use fire extinguishers which is a threat to library resources because they could not use a fire extinguisher in case fire broke out. *"Library management have never thought of taking us for a training on how to use a fire extinguisher as it is no one can manage to use it if fire broke out."* Observed one respondent. The findings showed that only respondents from three libraries indicated that they knew how to use a fire extinguisher. The findings further indicated that regardless of the type of portable fire extinguisher available, it was essential that every library installed this equipment for extinguishing small fires.

Respondents were asked to state the effectiveness of fire extinguishers that were installed in libraries. The findings clearly indicated that all the libraries under study realized the need to

install fire extiquishers. However, it emerged that only few libraries had fire extinguishers that were effective because they were frequently serviced and were used before to quench small fires. It was also revealed a lot of libraries did not service their fire extinguishers. This is an indication that extinguishers in these libraries were not in position to do a better job. Library management should always ensure that their fire extinguishers are serviced every time and again if they are to be effective and reliable.

4.5.4 Non-return of borrowed books

The study sought to find out the security measures that were put in place when borrowed books were not returned, respondents were asked. The study indicated that libraries had put in place some security measures to books that were not returned and the following were security measures put in place: The findings revealed that respondents from many libraries indicated that, borrowers were charged a penalty fee for not returning books and other library items on time, while respondents from only one library indicated that they did not charge a penalty fee. One respondent mentioned that: "*A penalty fee is slapped on a user who doesn't bring the book on time.* "*We charge them for bringing books late so that they learn to bring books on time because this will help other library users to access the same books*; *the amount is determined by the number of days the borrower has exceeded the due date*".

The study further revealed that more than half of the libraries called them or sent emails to defaulters to remind them to return the books**.** One respondent stated that: "*We either call the borrower or write them a reminder about the unreturned books or follow them physically if they are within reach."* Respondents from a few libraries indicated that they did not use this method as a way of reminding borrowers to bring back the books to the library. It was also found that many libraries did not clear those who did not return library books at the end of the semester. The results showed that when borrowers have not cleared this forces them to return the books they borrowed in fear of not getting cleared. It was further showed that respondents from the majority of libraries indicated that they did not use amnesty week to have the books returned, while respondents from the many libraries indicated that they used amnesty week to ensure that all the unreturned books were brought back to the library without being charged a penalty fee.

The study sought to find out the effective security measures that were put in place when borrowed books were not returned. Most libraries indicated that the charging of a penalty fee for books not return and was effective because several library books had been returned after

the introduction of the penalty fee. The results further showed that borrowers were scared to pay a penalty fee and this forced them to return books for fear of not getting cleared at the end of the semester. The study further that following up library members who did not return books by calling them to bring the books back was effective because a good number of books were recovered. Amnesty week also proved to be effective since during this week all those who did not return library books were encouraged to bring them back without a charge. However, the study revealed that respondents from a few libraries were of the view that the security systems were not effective because some books have not been returned after the measures were put in place.

4.5.5 Security Challenges Relating to the Library Entrance, Window, and Door

The study tried to establish a security measure that was put at the library entrance. The findings revealed that library users were required to produce their IDs when going into the library for easy identification. The findings revealed that many libraries did not experience a problem where staff and readers fail to present their IDs. While few libraries experienced a problem where users were not cooperative in presenting IDs at the entrance. It was further indicated that it was difficult to identify genuine library users when patrons did not present their IDs. One respondent mentioned that: "S*ome students and members of staff don't want to change to modern ways of managing library security and this hinders the progress in ensuring modern security worked well. They also don't like anything to do with checking in their bags when they leave the library*".

The study further revealed that ID cards had minimum details of an individual such as name, photo, school or name of the issuing department or organization, expiry date, and a unique card number such as computer number for students and man number for staff. The study also showed that when there was power failure it was difficult to check who was legible to access the library because some students would come claiming that they wanted to get their belongings which they had left inside. The findings also revealed that respondents from one library used gate register where users were required to sign in, in a logbook when entering in the library by writing down their names, ID number and also sign out when leaving the library. The study showed that gate registration was one way of screening true library members. The study further revealed that most libraries with a small number of library users used this method of registering or signing in a logbook. One respondent argued that: "*The library rules clearly states that library users when accessing the library and its resources should use their IDs. This makes it very easy to identify true library users and to prevent theft of library materials"*.

In trying to establish the measures that were put in place to avoid users borrowing books using someone else's ID, respondents were asked. The study revealed that more than half of the libraries indicated that they allow students to borrow books using someone else's ID as long as permission was granted, while respondents from few libraries indicated that they did not allow students to borrow using one's ID. The study further revealed that identity cards were confiscated when a user tried to borrow a book using someone else's ID and borrowers were also taken to a disciplinary committee when they were found using a friend's ID. One respondent mentioned that: *"We don't allow users to borrow books using someone's ID card for fear of losing library materials, we can easily tell from the photo on the ID since all the students are registered in the library with their faces captured*".

The study sought to find out the effectiveness of an ID as a security measure for accessing the library. The findings revealed that respondents from the majority of libraries indicated that IDs provided to staff and library users for identification were very effective, while respondents from few libraries indicated that they did not ask for IDs when accessing the library. The results showed that library users were screened at the entrance by checking IDs to see who was legible or not to use the library and this prevented unauthorized people from entering the library.

However, respondents from very few libraries showed that IDs were not effective because outsiders had managed to enter libraries and went way with library items. The results further revealed that library users were at times allowed to enter the library without an ID after convincing people at the entrance that they lost or misplaced their IDs and this compromised the security system. The results further revealed that in most cases people at the entrance did not compare the picture on an ID to the person accessing the library especially when the library was busy.

In trying to establish whether an ID was effective for borrowing books respondents from half of the libraries under study indicated that IDs were effective because library staff were able to identify the owner of an ID since identity cards had photos which helped them for easy identification and this could deter library users from using someone else's ID. The findings revealed that using someone else's ID to borrow library materials was not allowed for security reasons. One respondent mentioned that: "*An ID is a very effective security measure because, after its implementation, theft rate drastically dropped''.*

However, respondents from five libraries felt that the security measure was not effective because at times library staff were overwhelmed with work and did not check and compare the

photo on an identity card and that of a person borrowing, while respondents from three libraries show that they did not use IDs when lending out books but instead write down the names and details of the book. One respondent mentioned that: *"The measure is not effective because library users have continued using IDs for their friends. We have received complaints from users when they are told that there are books in their accounts and they would say I did not borrow those books someone just used my ID without my knowledge and some would say I lost my ID card a long time ago."*

The study further investigated the types of security measures that were put in place to mitigate library security problems that were faced by libraries of higher education institutions and respondents were asked about the one in charge of opening and locking the library and also the one handling the library keys after the library was closed for the day. The results showed that respondents from more than half of the libraries indicated that their libraries were opened and locked up by security officers together with library staff on duty who witnessed that the library was locked and keys were kept at the security office. While respondents from few libraries indicated that their libraries were locked and opened by a librarian on duty who also kept library keys after closing the library. One respondent mentioned that: "*A library can only open or close when both a security office and library staff are available."*

The results further indicated that respondents from a lot of libraries stated that, the security system was effective because libraries had not experienced a situation where keys were used to open the library outside normal working hours to steal library materials. However, the respondent from few libraries indicated that the security system was not effective because library keys were kept by a librarian and not at the security office. The findings further revealed that respondents had experienced a situation where a librarian opened the library at an augured hour and library materials were stolen through the use of library keys to open the door. One respondent said: ''*We suspect that keys have been used to steal library materials by opening the library outside normal working hours. For example, we have been losing computers in the library without any breaking in."*

The findings further revealed that library windows and doors were well protected from being used for theft of library materials. The results indicated that respondents from more than half of the libraries showed that their libraries had windows and doors protected with strong grill doors at the entrance, burglar bars, and mesh wire were also put on windows to prevent library users from throwing books through windows when stealing. The findings further revealed that when windows had no burglar bars thieves could easily gain entry into the library through the

windows especially at night and also when there was no mesh wire on library windows thieves could easily open the window and push library materials. The study further indicated that respondents from few libraries showed that they did not have mesh wire on their library windows.

The study sought to know the effectiveness of the burglar bars, mesh wire, and the grill door. Respondents from nine libraries indicated that doors with grill doors at the entrance and windows with burglar bars, and mesh wire were effective. The study revealed that libraries with burglar bars and mesh wire on their windows had not lost their library materials thrown through windows. This showed that burglar bars and mesh wire were effective. The results further showed that libraries with grill doors had never lost their materials through the entrance and this proved that grill doors were effective. However, one library that did not have mesh wire experienced a loss of its materials as users throw materials through the window. *" The library has been losing books by pushing them through the windows, especially in the night during power outages because there no mesh wire on the windows."* Said one respondent.

4.5.6 Security Guards

The study sought to interview security guards from nine libraries and were asked whether they were taking patrols in their libraries to see if library users were not doing any illegal activities. The findings revealed that respondents from most of the libraries indicated that they were not patrolling because their libraries were small and they were able to see all the activities happening from the entrance where they were stationed. The results also showed that respondents from two libraries revealed that, these libraries were too big for them to undertake library patrols as they were understaffed to provide security services to the library materials. The study further revealed that most libraries were understaffed of security officers, hence officers manning the libraries were unable to carry out patrols to check and ensure that no one was abusing the library resources, while respondents from two libraries indicated that they were doing some patrols. Security guards were also asked if they were trained for the job they were doing and the findings of the study revealed that all the security officers from nine libraries attended the training on security. "*The problem we have is that there are few security guards we have in the library and because of this they few we have are unable to take patrols and see what users are doing. We have been hoping that library management could employ more security guards so that some can be taking patrols"* One respondent said that.

Furthermore, the results showed that security guards were employed to take care of the library's assets such as people, books, and equipment from a range of dangers such as theft of library

materials, hazardous users' behavior, enforcing preventative measures. Respondents further indicated that security officers were placed at the entrance or exit point to make sure only library members were allowed to enter the library and also to ensure that no one got a library book out of the library without following the proper channel of borrowing books. The study further discovered that those who did not have security guards had small libraries. The results further indicated that a respondent from one library was working alone at the station to check library users going in and leaving the library. The results further showed that she/he was the one receiving and giving out bags at the cloakroom as well as to make sure that library users sign in and out in the logbook. It was also revealed that this respondent could work from 06:00 to 17:00 hours alone before another officer could come to take over. The physical observation was in line with the lamentation from the officer that the library was understaffed because true to her words, she was busy attending to students while being interviewed. This causes security threats to library resources as this officer could get tired and lose concentration on her duties. One respondent mentioned that: "*Security guards keep an eye at whomever as coming in and going out of the library to make sure that there is no one who goes out with unauthorized library property".*

The researcher further sought to know the effectiveness of security guards that were put in place as a security measure to library resources. The results showed that a lot of libraries were of the view that security guards were effective to protect materials from theft. This is because there was a reduction in the theft of library materials with the presence of security guards. The study further showed that security guards were trained and were able to identify library materials. The findings also revealed that security guards were able to check effectively for library materials even when there was no power other than any other security system. The results also indicated that a lot of libraries used security guards to protect library materials.

However, respondents from few libraries argued that security guards were not effective because they have continued losing resources. The results further revealed that security officers at times were corrupted by thieves for them to allow stolen books to pass. It was also revealed that security guards at times left their stations unmanned. The study further showed that security guards in most libraries did not take patrols in the library hence causing security threats to library resources. One respondent said that: *" Security guards in our library in most case leave the exit unmanned and users take this opportunity to smuggle library books,"*

4.5.7 Security of Staff and Library Users

To establish the security measure provided to library staff and library users, respondents were asked to state how libraries provided security to staff and library users. The results revealed that a lot of libraries provided security to staff and library users by having security personnel up to time when libraries closed, while respondents from few libraries had challenges because they were not provided with security guards in their libraries. The results also revealed that respondents from most of the libraries indicated that library staff were provided with transport to and from their various homes when working late, while respondents from few libraries indicated that transport money was given to a staff working late. The results further showed that respondents from three libraries indicated that those working late were given institutional houses within the premises to stay in. The results further indicated that fire extinguishers were installed in libraries of which library staff can use to protect themselves in case a fire broke out. *"Library management have really tried their best to provide security to library staff especially, those working in the night. Those working in the night have been provide transport taking them to their various homes."* One respondent said that.

The results of the study further revealed that respondents from most of the libraries indicated that the security measures were effective because safety was provided to them by providing security guards up to close down of the library and no negative issues happened. The results further showed that staff were provided with transport to and from their various homes when working late. The results further revealed that some libraries had allocated accommodation within the premises to staff working late.

However, respondents from few libraries were of the view that the security measures were not effective because library staff were harassed by readers when they wanted to close the library because there was no fuel to continue working after normal working hours. It was further revealed that transport for those working late at times was not available due to fuel problems or break down and at times the drivers came late to pick up staff after working late which made them reach home very late.

4.5.8 Types of Training Offered to Increase Staff and User Awareness on Security Issues

The study tried to find out if libraries had organized activities and training being offered to increase staff and user awareness of security issues. The findings of the study revealed that in fifteen libraries they had activities and trainings that were offered to increase staff and user awareness on security issues, while in one library there was no organized training done. When respondents were asked to state the types of training offered to increase security awareness.

The results of the study revealed that in nine libraries, it was done through orientation programmes, while in three libraries it was done through security sensitization and induction when school opens. The findings showed that in two libraries trainings and awareness were done by having workshops. *"The trainings have been helpful to both staff and library users because everyone is made aware of library security issues and the consequences of being found on the other side of law. This has really reduced theft of library materials."* One respondent observed that.

When asked how often these activities and trainings were conducted. The study revealed that in eight libraries training was conducted every semester, while in three libraries training was done when the need arises and at least two times a year in two libraries. The results further showed that training in two libraries was conducted at the beginning. When respondents were asked about who conducted this training. The study revealed that in fourteen libraries training was conducted by library staff, while in one library training was conducted by staff and security guards.

The study investigated whether libraries had put in place rules and procedures to access print materials, respondents were asked. The study revealed that all sixteen libraries had put in place rules and procedures to protect print materials. Respondents were further asked whether the rules and procedures were documented and understood by all the staff and library users. The findings revealed that in most libraries rules and procedures were clearly documented and understood by the users, while in few libraries the rules and procedures were not properly documented and understood by readers. The researcher requested to see the documents and it was physically observed that rules and procedures were documented in the library users' guide book which was given to users when they come for the first time. These rules were made clear to users through orientation when first-year students came for library orientation. Respondents were further asked to state the rules that were put in place in their libraries. The study revealed that the common rules in all the library's understudy were that readers were not allowed to enter the library with bags. They were also not allowed to carry food or water in the library and smoking was also not allowed in the library.

The study sought to know the rules and procedures that were put in place to access restricted areas like short loan collection, respondents were asked. The study revealed that in many libraries books in the short loan were in a closed access area to students which means readers can get books from the shelves through a member of staff. The results also showed that three

libraries did not have a short loan collection. The study also revealed that materials from this section were borrowed using an ID and were used within the library for a short period so that everyone could have access to them. For example, in one library books from this section were just borrowed for 2:30 minutes and also for overnight. "*No book will be borrowed without borrowers using an ID. Book can also be taken out overnight and students cannot access books on their own from shortloan, they have to borrow through a member of staff,"* said one respondent. Another respondent observed that "*short loan materials are lent out using IDs only for 24 hours".*

4.5.9 Problems Relating to Stocktaking and Detection of Security Threats

To establish if respondents took regular stock taking and report to ascertain total collections, to detect security threats, lost, misplaced, theft, respondents were asked to state their position. The results showed that more than half of libraries did not carry out stock taking, while few libraries took regular stock taking and report to ascertain total collection, detect security threats and misplaced materials. The results further revealed that in two libraries respondents were not sure if their libraries took stock taking. Those who did not take regular stock-taking were further asked how they knew the lost, misplaced and damaged materials and how frequently. The study revealed that seven libraries became aware of lost, misplaced, theft, and damaged items when a reader wanted to borrow that particular item and also through random checks. Respondents were further asked how regularly they carried out stock taking. The findings showed that three libraries carry out stocktaking at the beginning and end of the semester, two libraries showed quarterly, in one library it was done when the need arises. However, in one other library, it was done after six months*." Our library has a serious problem with stocktaking because from the time I joined this library no stocktaking has been carried to assess which books are on security threat or missing."* Said one respondent.

4.5.10 Different Personnel in Charge of Security Management in Libraries

In trying to establish the kind of security personnel in charge of security management in the libraries. The study revealed that in seven libraries, security guards were in charge of security management, while in five libraries library staff were in charge of security management. It was also revealed that in two libraries, the administration was in charge of security management by outsourcing a security firm. The results further revealed that in one library, the head of the security department was in charge. The results of the study also showed that in one library a security coordinator who is a lecturer was in charge. When asked further about the role they played, the findings revealed that they provided security services to library materials, staff, and

library users. They also organized security personnel and see to it that good services were delivered.

In trying to establish whether the security personnel had defined roles and responsibilities. The study revealed that security personnel had defined roles such as patrolling in the library, manning allocated places such as entrance and supervisors ensured that enough personnel was deployed to respective areas. One respondent mentioned that: "*Yes, the security personnel have defined roles such manning the check point and the exit. They know exactly what should be done and how to go about their daily routine duties"*.

The study further investigated whether libraries had security management team in their libraries. The findings of the study revealed that most of the libraries did not have a security management team and only one library had a security management team. The study further revealed that the security management team is very important to the library to ensure that the right and effective security systems are put in place to protect library resources. "*In our library we don't have a security management to oversee the security issues in the library and because of this we problems where anyone say anything on how to provide security in the library*." Said one respondent.

4.6 Electronic Security Measures Libraries have put in Place to Mitigate Against Security Problems

This section provides the findings regarding electronic security measures that were put in place to mitigate security problems libraries were facing. The results indicated that there were seven common electronic security measures used and they were presented in table 3 below ranked in descending order.

Table 4: Electronic security measures academic libraries have put in place to mitigate against security problems libraries are facing.

Ranking	Electronic security measures
1	CCTV camera
2	3M book detecting system
3	Antivirus software
4	Password
5	Alarm system
6	Smoke detector
9	Radiofrequency identification

4.6.1 Closed Circuit Television (CCTV Camera)

To establish the security measures that libraries have put in place to prevent library materials from theft and mutilation. The results from Table 4 above indicated that the a lot of libraries had closed circuit television (CCTV) cameras installed in their libraries as part of the security measure to ensure that print materials were protected from theft and mutilation. The physical observation of the surveillance cameras in these libraries showed that some libraries were installing cameras in all areas of the library, others only installed in areas which they thought were critical. The findings also revealed that respondents from five libraries did not have closed circuit television (CCTV) cameras in their libraries. Furthermore, the observation indicated that electronic security cameras were placed and positioned in areas where there was a high likely hood of some illegal activities. Respondents further indicated that the security measure was able to help security officers or library staff to monitor all the library activities. One respondent observed that: " *Before the installation of CCTVs in the library, a lot of books and journals used to go missing. But now it's rarely that books go missing. Therefore, I can safely say that the security system put in place is effective".*

The study sought to know the measures that were put in place to protect users' items in the cloakroom from theft. Respondents were asked how they ensured that user's items at the cloakroom were protected. The study revealed that respondents from a lot of libraries understudy stated that electronic security cameras were installed. While few libraries indicated that they did not install CCTV cameras to monitor the cloakroom. One respondent mentioned that: *"The installation of CCTV cameras in the library has enabled us to monitor the library activities effectively. This, in turn, has made users' items secure"*.

In trying to establish the measures that were put in place to prevent theft of computer equipment in libraries. Respondents from a lot of libraries indicated that they did not have CCTV cameras in their libraries, while respondents from a few of libraries revealed that their libraries installed with CCTV cameras in the computer lab and OPAC area. The measure was put in place to prevent theft of computers where so that are stopped from removing computer parts illegally that caused computer malfunction. The findings revealed that theft was seen as a threat to computers before the installation of security cameras because computers were physically damaged deliberately by users and some parts such as mice, keyboard, and a computer monitor were stolen and unauthorized downloading.

The study sought to know the effectiveness of the security measures that were put in place to protect library resources, respondents were asked to state the effectiveness of the CCTV cameras that were put in place as a security measure to protect computers. The **s**tudy showed that a lot of libraries had CCTV cameras which were quite effective because they were installed in the right places. The results also revealed that CCTV cameras in these libraries were regularly serviced. The study further revealed that in these libraries there was always a security guard or library staff in the monitoring room to watch activities going on in the library. The findings further revealed that in places where cameras were installed vandalism and theft of computer components were reported to have drastically reduced. One respondent mentioned that: *"The installation of close circuit television cameras have really helped us to reduce theft of library resources. We have apprehended library users before who have tried to vandalize our library computers".*

To prove the responses from respondents, the researcher obtained permission to observe how the closed-circuit cameras (CCTV) worked, and with the help of the library staff and the security officer on duty, the researcher was allowed to view different cameras to see the activities taking place in various sections of the libraries. The effectiveness of the CCTV cameras was tested further by taking a notebook in one of the sections of the library and removed some pages from it. Afterwards, the researcher with the security guard and staff went to the CCTV monitor room to playback the security systems, and the system showed the activity of removing pages from a notebook. This revealed that CCTV cameras were effective when they are installed in all areas of the library. The findings showed that if the security system was to be effective there was a need to have a security officer in the monitor room throughout to watch the activities happening in the library and CCTVs were supposed to be

installed in all the sections of the library. The study further revealed that maintenance of security systems was key to their effectiveness.

However, the results indicated that in few libraries closed circuit television (CCTV) cameras were not working due to lack of regular maintenance and this caused security threat to library resources. While in one library CCTV cameras were not effective because the library had continued missing computer components like mice, keyboard and computer monitor. The findings further revealed that in most cases there was no one in the surveillance control room to monitor what was happening in the library. A test to observe the effectiveness of closed circuit television (CCT) cameras was carried out from this particular library where pages from a notebook were removed from each section of the library. The observation showed that only the entrance, cloakroom, and circulation desk were captured by CCTV and the rest of the departments or study areas of this library were not installed with CCTV cameras which posed security threats to library materials. After testing the CCTV cameras by removing pages from a notebook in areas where they were installed, the researcher with the help of the security guard went to the monitor to play it back. The results revealed that the computer monitor in this particular library was defective as it kept on skipping most of the time and pictures were also poor. The results indicated that in this library CCTV cameras were not effective, cameras and computer monitors were defective and there was also no one to man the monitor room. One respondent mentioned that: "*Our computer monitor connected to CCTV cameras has a problem because most of the time it keeps on skipping when rewinding which is difficult to do our work properly".*

4.6.2. 3M Book Detection System

In establishing the security measures academic libraries had put in place to mitigate against security problems libraries were facing, respondents were asked. Table 4 above indicated that a lot of libraries had 3M book detection or 3M library security systems installed in their libraries as a security measure to library materials, while few libraries did not have a 3M book detection system in their libraries to prevent theft of print materials. The findings showed that 3M book detection systems were installed at the exit of the libraries. To confirm the findings physical observation was done to check if these libraries had 3M book detection systems. The results confirmed the responses from respondents to be true that some libraries had installed the devices. The study further revealed that the security system work in combination with magnetic security stripes inserted inside a book or on the spine of the book. The findings also revealed that borrowed books had to pass through an electromagnetic machine for desensitization so

that they do not set off an alarm or triggering when passing at the exit. The results further indicated that when books were returned, they were discharged from the system and there was a need to sensitize them so that the magnetic stripes were activated and trigger or produce a loud sound when someone passed through the exit with a stolen book. One respondent mentioned that: "*Yes, the 3M book detection machine is installed in the library but the challenge we have is that over the past two years the machine has not been working due to lack of maintenance. This has exposed our resources to theft*, even *this machine was bought as a measure to prevent books and other materials from being stolen.*"

To find out about the effectiveness of the 3M book detection security used by academic libraries understudy, respondents were asked how effective the 3M library security system and participant observation methods were also used to assess the effectiveness of electronic security system in most of the academic libraries. After the interviews, the researcher employed the participant observation method to assess how effective the electronic security systems were. After getting permission from library staff on duty to observe how effective the devices were. The researcher carried out an observation with the help of library staff and security personnel from seven libraries; the researcher took a book from a shelf and tried to pass through a 3M book detection system. True to the test done, the alarm system triggered. This confirmed that the electronic security devices in four libraries were effective. The findings of the study further revealed that the 3M library security system was very effective because the loss of library materials reduced after the installation. The study further revealed that many library users were intercepted when trying to pass through with stolen books. The study also indicates that the security system scared them because of the embarrassment they went through when it produced a loud sound that everyone could hear in the library. One respondent said that: "*The security device was quite useful, but the only challenge is that when power goes off it becomes inactive and users can take advantage of this to walk aware with library resources particularly in the night. Therefore, there is need for management to install a generator so that even in absence electricity the security system can remain active."*

After the testing of the 3M book detection system through observation method from three libraries. The results of the test revealed that the 3M book detection systems installed in these libraries were not working for several years due to poor maintenance and this made them ineffective and these libraries had continued losing library items. The findings of the study further indicated that the security system became inactive when there was no power which led to the loss of books because it could not detect stolen books.

4.6.3 Antivirus Software

In establishing the security measures that were put in place to mitigate computer-based information problems such as hacking and cracking institutional networks, respondents were asked. Table 4 above revealed that a lot of libraries installed antivirus software, firewalls as well as close monitoring to the use of computers. The results further indicated that anti-virus software prevented computers from being attacked with viruses and computers were regularly updated. The findings also showed that firewalls helped to protect the computer network from being attacked by hackers, crackers so that they do not access institutional information**.** Respondents also indicated that they lost data due to the use of flash drives that were affected by viruses, computer crashed and sometimes data was lost mysteriously.*"Yes, antivirus software was installed so that computers are protected from being attacked with computer viruses and this have prevented loss of information from computers."* Said one respondent.

In establishing the effectiveness of measures that were put in place to ensure the security of the computer-based information systems, respondents were asked about the effectiveness of the antivirus software, firewalls, and close monitoring. The study revealed that the antivirus used in more than half of the libraries were very effective because they had not experienced any problems where a computer crashed or hacking of the system. The results also indicated that the anti-virus software prevented computers from computer viruses and these computers were regularly updated.

However, the results showed that the antivirus used in few libraries were not effective because computers were in most cases affected with computer viruses and were not regularly updated by ICT staff, since they did not have well-trained staff stationed in the library. The study further revealed that libraries had lost some important data due to computer clashes and computers were very slow. One respondent said that: *" Our computers have been attacked with antiviruses before, this could be due to the ineffectiveness of the antivirus software installed and also due to lack of updating computers regularly."*

4.6.4 Passwords

In trying to find out the security measures that were put in place to protect information resources, respondents were asked. The study revealed that respondents from a lot of libraries indicated that technical measures such as user name and passwords were put in place to protect information resources as presented in Table 4 above. However, respondents from few libraries indicated that they did not use passwords. The results further revealed that the use of a password was the most basic form used to ensure that only authorized people accessed confidential data

and the databases. It was also revealed from the study that strong passwords were required to ensure that other people could not guess the passwords and passwords were not supposed to be written on a piece of paper because other people might see it. The findings further revealed that passwords were supposed to be changed every after three months for security reasons. One respondent said that: "*Our staff uses passwords to prevent unauthorized people from accessing confidential information. Apart from accessing confidential information important files can also be deleted and therefore, we urge our staff to be using strong passwords which need to be changed regularly and keep them as a secret."*

The study further revealed that all the server rooms had controlled access as the keys to this room were only handled by people who were in charge of that place. The study also showed that there was control in the use of computers in offices as each staff was given a password to use and in some libraries, computers were set in the way that if the computer was not used for ten minutes all so the computer would shut down to prevent unauthorized people from accessing information when the owner of the station or office happened to leave the place with the computer on.

In trying to assess the effectiveness of the security systems put in place to protect information resources on computers, respondents were asked to state the effectiveness of the use of passwords and accounts for staff. A lot of libraries showed that the passwords used were effective because no complaint was received indicating that a different person managed to steal the password and used it to access confidential information. The findings further revealed that these libraries used passwords that were difficult to guess and the passwords are not shared. The study showed that these libraries changed passwords every three months, while four libraries do not use passwords. However, only a few libraries showed that the passwords used were not effective because people have managed to access confidential information or records. When asked further the reason why they think the passwords used were not effective. The results showed that passwords sharing among the library staff were common. The study further revealed that some members of staff write down their passwords on pieces of paper for fear of forgetting the password and leave the paper carelessly on their tables. The findings further revealed that some libraries were not changing passwords frequently. *"The passwords used in this library are not effective because we have heard some people complaining of having lost confidential information and some do not use passwords at all. I think there is need for library management to make it mandatory and ensure that everyone uses passwords as this will help to control deletion and accessing confidential information."*

4.6.5 Alarm System

In trying to find out the security measures that were put in place to protect library resources, respondents were asked. The findings revealed that respondents from many libraries indicated that they did not have alarm systems in their libraries. Table 4 above indicated that few libraries installed alarm systems to provide security. The study further revealed that an alarm system produced an audible, visual, or other forms of an alarm signal when it was tempered with an intruder, and this scared thieves away (Ezeabasili, 2018). The findings also showed that alarm systems were intended to restrict and control the physical access of people to the library, hence proving security measures to library materials. One respondent said that: " *Yes, an alarm system was installed in the library and it has helped us a lot because so many time we have been alerted. I remember one night around 02 hours thieves tried to break in and they could not go in because of the alarm system."*

The results further indicated that few libraries that installed alarm systems showed that an alarm system was very effective. The study also revealed that sensors were placed at the door or windows of the library. The findings further showed that an alarm system was quite effective because when a person tempered with the window where it was installed it produced an audible, visual, and alarm signal scaring away an intruder. The study also revealed that the gadget prevented intruders from illegally entering the library and it was always left activated when the library closed down for the day. One respondent said that: *" when we close the library we ensure that the alarm system is activated so that intruders are prevent from entering the library."*

The findings further showed that alarm systems installed in two libraries were not effective because thieves have managed to break in and store library materials. The study discovered that the security systems installed in these libraries were not serviced from the time they were installed which made them not perform well.

4.6.6 Smoke Detectors

In trying to find out the security measures that were put in place to protect library materials from fire, respondents were asked. The study revealed that more than half of the libraries did not have smoke detectors. The findings revealed as presented in Table 4 above that only a few libraries had installed smoke detectors. After taking closer observation the findings showed that these libraries installed the devices in almost all parts of the libraries. The study also revealed that a smoke detector was able to detect the smoke as soon as fire in the building starts. The findings further revealed that when there was smoke, the smoke reacted to it by

producing a visual or audible signal which alerted the occupants of the building. The findings also revealed that automatic smoke detectors were installed in the ceiling for early detection of smoke and notify occupants through sounding an alarm. Smoke detectors normally were connected to a central panel which was connected to the fire department so that firefighters could easily be notified. The study further revealed that smoke detectors were supposed to be installed in all hallways and to confined spaces in the building, and above potential fire hazards (Ezeabasili, 2018). "*Our library is installed with smoke detectors that have been effective because every time when there is smoke in the library the devices would give a signal. These security systems are installed in different areas of the library so that fire can easily detected."* One respondent lamented.

The study further revealed that respondents from most of the libraries indicated that they did not have smoke detectors in their libraries, while respondents from four libraries indicated that smoke detectors were quite effective because they have detected smoke before immediately it started coming out and a signal or alarm was given. *" It is unfortunately that library management have never thought of acquiring this important garget. Anyway am not sure maybe they are lacking some funds to purchase one."* Said one respondent

Respondents from few libraries that installed smoke detectors indicated the devices were effective. The findings established that the gadgets have managed to alert them every time there was smoke in their libraries. Further, it emerged from the study that the installation of smoke detectors in all areas or sections of the library and regular sercing contributed to their effectiveness.

4.6.7 Types of Training Focusing on Security in Database Management

The study sought to establish whether libraries had training focusing on security in database management, respondents were asked to indicate whether or not they have attended a any training focusing on security in database management. The study revealed that respondents from most of the libraries attended database management training that could offer an opportunity for them to get familiar with library information systems. The findings further revealed that respondents from a few libraries did not attend database management training, while respondents from other libraries showed that they were trained in database management systems. One respondent observed that: "Usually *I attend information systems training and database management training when the need arises*".

Those who did not have any training were further asked what they had done towards this goal. The study revealed that respondents had made suggestions to management towards having the training on database management. One respondent mentioned that: "*I suggested and submitted to management for consideration for training*". "*It's very important to be trained because knowledge can enhance security consciousness*".

In establishing the effectiveness of the security systems that were put in place for effective service delivery, respondents were asked whether the training in library and database management was effective. The study revealed that the trainings conducted in most of the libraries were effective because they understand the ICT issues without problems and therefore, they had a better understanding of database management. The study further revealed that these libraries had never experienced computer problems from the time the staff attended the training. The results of the study discovered that the training was important and effective. However, the findings of the study revealed that the training conducted from a few libraries was not effective because they had just attended workshops and seminars on ICT for a few days. One respondent lamented that: *" The trainings we have attended have been very effective as we have better understanding of ICT issues and our library has been always safe in terms computer related issues."*

4.6.8 Generator

The study sought to know the measure that was put in place to protect library materials when power went off, especially in the night. The results indicated that respondents from alot of libraries did not install generators in their libraries, while respondents from a few libraries revealed that they had power backups or generators installed in their libraries. The findings also revealed that generators switched on automatically when the power went off to light up the library immediately.

The findings further revealed that security officers physically check for library materials when a library decided to close due to a power outage. Furthermore, the study revealed that respondents from those libraries which did not have generators used to charge up lamps when the power went off in the night to light up the exit and ensure users are checked as they go out. Respondents from two libraries further indicated that generators in their libraries could run for long hours to support library activities, while respondents from two libraries showed that generators could not run for a long time due to fuel problems. The study also revealed that respondents from more than half of the libraries revealed that UPS was installed and used as a security measure for ensuring data saving when the power went off, while the minority of

libraries did not have UPS. One respondent mentioned that: *We use a generator to light up the library while the security officers keep an eye on them when leaving the library."*

The findings of the study further showed that respondents from three libraries were of the view that the security measure was very effective because normal library operations continued when the power went off. *"When power goes off there are high chance of library losing the materials because all the security systems becomes paralyzed as they depend on power. The problem is worse in the nigh because it is difficult for security guards and library staff to check and control users when power goes."* One respondent observed that. The results revealed that normal operations like charging and discharging library materials continued even when the power went off. However, the results showed that respondents from one library indicated that the security measure was not effective as it would happen that there was no diesel in the generator most of the time. The study also revealed that in this library the generator only provided light at the entrance and the issue desk which leaves other floors in darkness.

4.6.9 Radio Frequency Identification

The findings of the study showed that almost all the libraries did not install radio frequency identification in their libraries, while respondents from one library stated that a radio frequency identification (RFID) was installed in the library as shown in Table 4 above. The study further revealed that the device only allowed people who were provided with special tags to accessing the library. The security system also helps to track down library materials. One respondent observed that: "*One good thing about RFID systems is that the tags/transponders helped in tracking library materials. It can track the movement of a book or the person carrying it."*

The study further revealed that radio frequency identification (RFID) was effective because it controlled access to the library to those who did not have cards and only permitted accredited people were allowed to enter the library. The results of the study revealed that the system had reduced the loss of books by providing an effective detection system that tracked the number of library materials. One respondent said that: "*Radio frequency identification is quite useful it has managed to prevent intruders from accessing the library and also tracked a number of library materials."*

4.7 Suggestions to Overcome Some Challenges

Further in open-ended questions, respondents were asked to suggest the best way to overcome the challenges which libraries are facing. In their contributions the study revealed the following suggestion which were listed according to how common they are: managements should support

libraries purchasing security systems if they are to be effective by providing funds; management must ensure that there is enough security personnel in libraries; there is need to install CCTVs in all corners of libraries if the security system is to effective; there is need for libraries to come up with library policies that covers how security issues should be handled; there is need for library staff to be trained ; a library should come up with security management team to be looking into the affairs of security systems; libraries should be closing when there is power outages to avoid theft and mutilation of library resources; libraries should install generators, solar panels and UPS to be used when there is power outage; there is also need for libraries to start offering online services by subscribing to some databases like Jstor, Emerald and many others. There is also need to digitize library materials as this can prevent theft and mutilation of library materials, training of staff in charge of ICT department is required and it is also important that library staff are provided with transport to and from when working late.

4.8 Summary of the Findings

The findings of the study revealed that there were different types of security problems being faced by academic libraries in Zambia. The total number of 28 out of 45 elements participated in the study which comprised of both colleges and universities.

The study observed that libraries experienced a lot of challenges which included theft of library materials, book mutilation, power outages, vandalism, and unauthorized access. The causes of theft of print materials was due to lack of enough security personnel to man the libraries. Libraries have continued losing their resources because they do not have electronic security systems in place due to lack of funds. Those who have security systems are not working properly due to lack of regular maintenance. The effects of losing print library resources is that libraries tend to spend huge sums of money replacing lost materials. Another effect is that library users are denied an opportunity to have access to useful resources.

The findings further indicated that there were five major methods of illegal removal of library materials from the library such as concealing of books in clothes and this came out as the most common way of stealing library materials. The findings showed that this method is common in libraries that do not have proper security systems in place. Other methods include pushing books through windows when they do not have mesh wire; through impersonation; hiding books in bags.

The study revealed that a lot of libraries face theft of computer equipment and their peripherals like keyboard and mice. The results further showed that most libraries did not have competent

staff to handle the security of the information systems. It was also revealed that more than half of the libraries did not have written policies pertaining to information security. Other issues are to do with poor maintenance of ICT infrastructure, password sharing by library staff; installation of ineffective antivirus software are some of the problems.

The study has also revealed that the security measures that have been put in place include; the installation of CCTV cameras, alarm systems, 3M book detecting system, smoke detectors and fire extinguishers. Security guards have been also deployed at the library exist, use of IDs when entering the library and borrowing library books, purchase of generators in case of power outages, installation of ant viruses on the computer and putting passwords on the computers. Furthermore, the study also revealed that the security measures put in place were effective although some argued out that the security measures put in place were not effective.

CHAPTER FIVE: INTERPRETATION AND DISCUSSION OF THE RESEARCH FINDINGS

5.0 Overview

This chapter discusses the findings of the study presented in chapter 4 and it also discusses the findings according to the research objectives and questions. The study sought to answer the following research questions:

i. what are the types of security problems faced by libraries of higher learning institution in Zambia?
ii. what are the security measures academic libraries have put in place to mitigate against the security problem they face?
iii. how effective are the security systems in the academic libraries understudy?

5.1 Types of Security problems over Library Collections in Zambia

The first research question was to find out the types of security problems being faced by academic libraries in Zambia. The findings presented in section 4.3.1 of chapter 4 indicated that all the fifteen libraries experienced vandalism, mutilation and theft of print materials such as books by users. The results of this study conformed with Idris, Hassan and Abdul-Qadir (2013) who observed the incidences of book theft in libraries of higher institutions of learning. These libraries face security problem due to lack of enough security personnel to man the library. For example, if the entrance of the library is left unattended to this can allow unscrupulous people to enter the library and go away with library materials. Another reason is due to rapid growth in the size of a library collection. This has result in a sharp increase in security problems. Further, when print materials are not inscribed properly with ownership stamp. This can make libraries continue losing their resources especially when they do not have electronic security systems in place. The effect of losing print materials is that it become a drawback replacing lost materials because this money can be used for other developmental issues. The other effect is that library users are denied an opportunity to have access to materials when they want to conduct their research.

The findings further revealed that power outage make security systems become nonfunctional, thereby, creating danger on library materials. Library users can use this as an opportunity to steal library materials, especially at night because security guards find it difficult to check for library materials at the checkpoint as users leave the library. This happen to libraries without generators or charged up lamps. Consequently, libraries need to put up a standby generator in

case of power outages so that electronic security systems can continue with their normal operations. This can help to prevent theft of library resources and also ensure that other library services are not disrupted.

The findings revealed that libraries experiencing mutilation of print material because of poor security in these libraries. The findings of the study were in line with Mansfield (2009 who reported on book mutilation in libraries. The reason for these libraries to have continued facing mutilation of print materials was due to lack of insufficient funds to purchase electronic security systems such as CCTV cameras which could monitor all activities in the library. Another reason is that those libraries which have installed the surveillance system did not install them in all areas of the library; this leaves places not installed prone to mutilation and also it could be because the devices are not serviced and maintained regularly which makes them not functioning well.

The reason why these libraries experienced mutilation of print materials is because they are difficult to find as they are in short supply and when they are found they are expensive to buy. This makes these materials to be on-demand where many readers are competing for one copy. For example, in most cases, libraries acquire only one copy of a journal title, volume, and issue and this makes such materials to be on-demand. When a material is on-demand readers tend to be selfish by wanting to have that material by themselves which in turn force them to mutilate the material. The findings of the study were in agreement with Isebe (2014) who stated that mutilators have high pressure to succeed in academic environment and this motivated most mutilation. The effects of this are that patrons are unable to find the needed information from the materials which makes a library a white elephant.

According to the findings, libraries face some challenges in ensuring library security. The findings in section 4.4.1 indicate that a lot of libraries did not receive adequate funding for security systems from top management. The results of the study agree with Abioye and Rasaki (2013) who indicated that insufficient funding of libraries of higher institutions of learning in Africa expose these libraries to crimes. Since crimes cannot be exterminated, prevention must be focused on through operative security where guards are employed to take care of the resources. This explains that insufficient funding makes it difficult for libraries to implement stringent measures to secure the library's collection and protect users as well as staff. The reason why libraries are experiencing the problem of funding is because of management failure to realise the importance of library security. Another reason is due to lack of policies to guide

on how to protect the already acquired library materials. When policies are put place, they could always remind library administrators and top management at large to secure funds for purchasing and maintenance of the security systems.

The findings revealed that more than half of the libraries did not have written policies and programs regarding library security. The findings are similar to the study by Adekunle**,** Adekunjo and Unuabor (2018) who revealed that the vast majority of libraries had no written security policy. The problem of libraries not having policies was caused by lack of zeal from library managers who are supposed to pursue top management to come up with a policy that covers security management. The other reason is due to lack of interest from higher authorities as they see it not necessary to have policies regarding better ways of providing security to library resources. The problem of not having a policy towards security systems is that there is no guidance as to how things must be done to provide library security. Library policy is important in the sense that it guides on how best to protect library materials. When a library has no policy this means that security problems will be resolved haphazardly as they come because there are no stipulated rules as to how to solve the problems when they arise. Therefore, libraries must create written security documents to guide library staff on how to provide security to library resources.

The findings showed that very few libraries had written policies and programmes on security management for information systems. The reason for these libraries to have come up with policies is because they realized importance of having a security policy. This is very good because the policy becomes a reference tool when providing security to the management of information systems (Ashenden, 2008). Since it's a reference tool it can also help to guide newly employed staff to follow the standard way of providing security. Library management should always ensure that policies are made available and accessible to all library staff so that they can work within the policy requirement. Policies must be accessible so that it can be used as a reference tool to new users when need arises. The problem of not having access to the policy is that staff may not use it for making the right decisions and also there will be no standard way of doing things in the library. The study further revealed that only respondents from one library indicated that the policy was accessible. This is a good thing because the staff will always make a decision based on the policy.

5.2 Security Measures Libraries of Higher Institutions of learning have put in Place to Mitigate Against Security Problems they face.

The study revealed some common security measures that libraries of higher institutions of learning have put in place some to protect their library resources such as inscription of library materials. The findings of the study revealed that all the libraries inscribed their materials with ownership stamps. Libraries thought of putting protective measures in place because they realized that inscribed materials with institutional stamp cannot be stolen easily. Apart from preventing materials from stealing this also help to identify their materials easily. Inscribing library materials is very important in the sense that it shows the institution which owns the material. The findings further revealed that accession numbers generated using information management systems are also used in some libraries as security measures. This also play an important role as it ensure that each item bear a unique number for easy identification. Each library material must have this unique identification number so that it can easily be identified from the rest. The findings of the study are in line with Oghenetega, Emojorho and Omah (2018) who reported on the use of institutional ownership stamps on specific pages of security pages as security measures.

The study showed that all libraries understudy had cloakrooms or at least a locker/cabinet which is a designated area for safekeeping users' belongings. Libraries came up with such a measure due to the fear that patrons were going to be using bags to smuggle library materials. This also help to prevent users from carry water, food, and even dangerous weapons that are not allowed in the library. Water is prohibit in libraries because they fear that it can spill on books and stain print materials. Water destroys books when it spills on them and other print materials that make pages stick to each other when drying them up. This also makes words to be unreadable eventually libraries are forced to spend money unnecessarily replacing such materials (Olugbenga & Elizabeth, 2011). While the reason why food was not allowed in the library was that food particles would attract rodents or insects which can eat and stain books with their droppings. Therefore, libraries must put strict rules to stop users from entering the library with their food and water so that print materials are protected from such dangers.

The findings in chapter 4, established that all selected libraries installed fire extinguishers in their libraries. This was due to libraries having recognized the problem which fire can cause to library materials. Libraries need to prepare themselves in advance to quench any fire outbreak. The findings of this study were in agreement with Eisenberg and Lawthers, (2005) who also encouraged the use of fire extinguisher to protect library materials against physical damage due

to fire. Man-made problems like smoking and cooking should be stopped in the library as they are the major causes of fire.

It emerged from the findings that a lot of library staff do not know how to use fire extinguishers. This is because most of the staff were not trained on how to use fire extinguishers. The problem is that library administrators assume that staff will automatically know how to use an extinguisher immediately they are employed which is not the case. This is a threat to library resources because library staff cannot manage to use a fire extinguisher in case a fire broke out. It is, therefore, necessary for all library staff to be trained on how to use fire extinguishers so that whoever is on duty can quench small fire rather than waiting for fire brigade. The fire fighter might take long to come as this may allow fire to spread to the entire library.

The results of the study revealed that a lot of libraries charged penalty fees for not returning books on time. The findings of the study agree with Mansfield (2009), who identified abuse of books which includes non-return of borrowed items. The results showed that users have the tendance of keeping overdue books. One of the motives for keeping books is to steal library materials, especially when books are on-demand and short supply (Fasae & Adedokun, 2016). Library users fail to return books if they are misplaced and when they want to continue using the books when they have not finished using them. This happens especially, if they know that they have renewed them more than the number of times required and cannot be allowed to renew them again. The results from the findings showed that respondents from one library did not charge a penalty fee. The reason for not charging users when they bring books late was due to the fact that the library has few students and have enough copies for users. The results further showed that few libraries use amnesty week to have the books returned. The whole idea for libraries to come up with this week was to ensure that those who did not have money to pay fine for keeping overdue books can take them back without a charge. This confirms the findings of Oyewusi and Oyeboade (2009) who recommended several steps for libraries to improve security by encouraging the use of general amnesty week. This should be instituted by all libraries in order to allow stolen books to be returned. Offenders must be dismissed or expelled from using the library.

Section 4.7.4 showed that a lot of libraries were asking users to produce their identity cards (IDs) at the entrance when entering the library. The findings were in agreement with Basaka et al (2020), who conducted a study in Nigeria on the introduction of identification cards to users. The reason for presentation of identity cards at the entrance was due to the fact that

libraries noticed that there was poor security at the entrance as anyone would enter the library without scrutiny. Library management also realized that a lot of materials were missing because there was no control at the entrance. The design of a libraries building also play an important role in the sense a library with one entrance and exist is easy to mange. This is in line with a study conducted by (Carey, 2008), who stated that the design of entrances and exits of the library buildings with only one exit appeared to be more successful in preventing theft. This is because buildings with one entrance and exit are easier to monitor and check for identification cards. This also helps to reduce the number of security officers to be employed to man the entrance and exit.

The study revealed that a lot of libraries had security guards. These institutions employed security guaars because they realized that they cannot do without physical security as security officers can remain active even when power goes off. This is different from electronic security that is dependent on power for it to function. Respondents from many libraries indicated that they were not patrolling. The reason is that libraries were understaffed with security officers. Therefore, officers manning the libraries were unable to carry out patrols to check and ensure that no one was abusing the library resources. This implies that they cannot leave critical areas like the exit or entrance unmanned because thieves can take their absence as an advantage to sneak in and smuggle the materials. However, officers in few libraries indicated that they were carrying out patrols. These libraries were able to carry out routine patrols because they have enough security personnel deployed and every library must strive to do so. The advantage of patrolling is that it instills fear to library readers from doing wrong things. The findings further showed that officers were trained for the job they were doing. The reason that led for these institutions to employ trained security guards is that trained officers have the skills of handling security issues unlike employing someone who is not trained. Libraries therefore should be encouraged to employ trained security officers as this will give a guarantee on the protection of the resources.

As shown in section 4.5.9 almost all the libraries had activities and training that were offered to increase staff and user awareness on security issues. The findings of the study is in line with Shamsul et al (2012), who carried an empirical study on how library trained personnel can influence library security. Library staff who are not familiar with security techniques are unable to implement security measures deligently. The findings also revealed that in most libraries user awareness was done through orientation programs, workshops, security sensitization, and induction when schools open. For this to be done library management

realized the need for training or orienting these people so that they are aware of the need to protect the materials. It is also done on grounds that they should know the consequences of being found on the other side of the law. This is good because it makes everyone to be conscious of security matters in the library and by doing so materials are protected from being abused. Therefore, this concludes that library staff should be given extensive security training so that they are familiar with security policies and security techniques.

The findings showed that all the libraries had put in place rules and procedures to protect print materials in restricted areas. These libraries made sure that such places are kept as closed access area to readers. This means that readers can only get books from the shelves through a member of staff. This is consistent with Purtell (2007), who indicated that closed access can prevent theft of rare materials by restricting access to these materials. Libraries came up with restricted areas in order to ensure that all rare and valuable materials are used within the library. Another reason for putting rules and procedures to restricted areas is to ensure that these materials are closely monitored so that they are not abused. The problem is that some users might not feel free to use such mterials. The rules and procedures put in place must be reliable and effective for the accessibility of such collections so that users again are not denied an opportunity to use the materials. This can also be enhanced by proper supervision and control of the library environment, especially designated places for such collections. Access to these areas must be clearly defined and regulated because this will help patrons to fully use the resources. There is also a need for staff to enforce restrictions by challenging users in a non-confrontational manner when they do not have what it takes to access materials from this area.

Apart from the use physical security measures, some libraries of higher institutions of learning have deployed electronic security measures to mitigate against security problems. The findings revealed that quite a number of libraries installed CCTV cameras as a measure to ensure that their resources are protected from vandalism, theft and mutilation. It is a fact that most libraries are now using technology so that their work become easier and efficient. It is for this reason that these libraries opted to use surveillance cameras to reduce the abuse of library materials. This confirms the findings from the study conducted by Merete, Albrechtsen and Hovden (2008), who surveyed on libraries that had electronic security systems in the United States of America. The results showed that the installation of electronic security systems can reduce mutilation and book theft. The use of cameras is quite helpful especially if they are installed in all areas of the library unlike selecting places where to install them. This is because once users realize that other places are not installed with cameras they can take advantage to abuse

materials from such places. For closed-circuit television cameras to be effective there is need to have a security officer in the monitor room to observe the activities of users and follow up those doing illegal activities. When user come to know that there are cameras installed in the library this instills fear in them hence reduce abuse of the materials.

The findings further revealed that few libraries did not have CCTV cameras in their libraries. The reason is because these libraries are lacking funds to purchase the cameras. Another reason is that these libraries are still believing in doing things in the old way and are hesitant to embrace technology. The problem of relying on physical way of providing security is that officers can leave the station unmanned and they can also easily corrupted. Therefore, It will be necessary to see these libraries embrace the use of technology such as CCTV cameras in preventing theft of their resources. The advantage of using a camera is that it does not require a large number of people for it to operate which gives staff to do other important things. Electronic security cameras were placed and positioned in areas where there was a high likelihood of some illegal activities. The reason is that these areas have high crime rate than any other area and management thought it was important to install cameras in order to prevent theft. It is important to note that the use of cameras should be adequately supported by security personnel just to amplify library security.

The results in Table 4 indicated that a lot of libraries installed 3M book detection systems as a security measure to library materials. The installation of this security system was done due to the heavy loss of library books and other print materials which libraries have been facing. These libraries realized that a lot of money was spent on replacing stolen books. To successfully mitigate theft of library materials the 3M detection system should be installed at the exit of the library. The library must have only one exit so that everyone leaving the library is screened. There is also a need to make sure that the security stripes inserted in books or print materials are not disclosed to users where they are embedded so that they do not temper with them. The challenge comes in if users come to know where the magnetic stripes are placed. This is because they can simply remove the stripe and walk away with the material. As typically only one security stripe is placed in each item, the removal of a stripe can be successful enough to defeat the electronic security system.

Furthermore, it is also important that librarians do not forget to pass returned books through an electromagnetic machine for sensitization so that the magnetic stripes are activated. When a stripe is activated this make the device trigger or produce loud sound when someone pass through the exit with a stolen book. If books are not sensitized after they have been discharged

patrons can easily smuggle the materials without being detected. The other problem that can make this device seem as though it is not efficient is when the user deviates from the security gate. This is most likely to happen when there is no security guard at the security gate. To minimize this problem there is need to ensure that a security officer is always available at the checkpoint so that no user avoids passing through the security gate.The findings revealed that that the security system become inactive when there is no power and this can lead to loss of books as the system cannot detect stolen books. In this technology-driven era, there is a need for libraries to invest in solar energy so that when power goes solar system can automatically switch on and provide energy to the security system.

The findings further revealed that few libraries did not install 3M book detection systems in their libraries. The reason this is that these libraries are lacking funds to purchase the devices because they are quite expensive. Another reason is that these libraries have a small number of users and they do not experience a lot of theft which makes management feel it is a share waste of money to buy expensive gadgets. These libraries should be encouraged to acquire this security system so that they secure their resources which are difficult to replace when they are lost due to insufficient funds. Even though this technological security system is expensive to buy, libraries must purchase to avoid theft and replacing of the resource every now and then which is more expensive. It is not a secret that the lost resources take long to have then replaced and this leaves users suffering.

The findings revealed that more than half of the libraries did not have alarm systems in their libraries. These libraries did not install alarm systems because of inadeguate funding for purchasing the gadget. The other reason is that these libraries have not realized the usefulness of this device. The advantage of using an alarm system is that it produces an audible or signal when it is tempered with an intruder and this sound scares thieves away. When users realize that there is a security device installed, this automatically instills fear and deter users from engaging themselves into illegal activities.

The benefit which is attached to libraries with an alarm system is the ability to be monitored remotely by professionals. The problem only comes in if the device develops a faulty and the expertise that installed the system stays far from the institution as this may take longer to repair the gadget. This can only be resolved by training local staff who should have the expertise to install and repair the system. However, few libraries installed alarm systems to provide security to library materials. These libraries recognised the need to secure the entry points, windows and doors, as well as the interior where valuables like computers and server rooms

are found. Regardless of the size of the library and its collections, the number of windows and doors, there is a need to install this device so that library resources are protected.

The study showed that a lot of libraries did not have smoke detectors. The reason is due to lack of funds by management to purchase the smoke detectors. Another factor is that planners or administrators did not see the need to install smoke detectors. Libraries without smoke detectors risk having their resources destroyed by fire because since fire cannot be detected at its inception and put it off when it is still small. This tool can alert occupants in the building immediately after smoke starts as it reacts automatically to smoke by producing a visual or audible signal. There is a need for top management to secure funds so that libraries can purchase this appliance and install it for early detection of fire.

The findings as presented in section 4.6.11 showed that a lot libraries did not install radio frequency identification**.** Management must secure this technology because the equipment has two major functions such as to circulate library materials and provide theft detection services. The findings of study are in agreement with Ali (2016) who studied library book theft and the use of radio frequency identification at the University Libraries of Pakistan. The study highlighted that most libraries did not use RFID technology for the security of their books. These libraries have not realized the benefits that come with the installation of this device such as to identify and track down library materials from a distance as long as they have tags. The system provides an opportunity for patrons to check-out/check-in library materials by themselves that gives library staff time to attend to other issues. Therefore, the device can improve customer services since it reduces the precious time that borrowers would have spent in the queue when borrowing or returning books. The gadget also help to easily identify print materials for the shelving process.

The findings indicated that only one library installed radio frequency identification (RFID). The reason for this library to have installed the device is because library management recognised the need to improve security of library materials. This gadget is used for tracking, charging, discharging, stocktaking and sort out the reading materials. The gadget has the ability to improve library transactions, improving services delivery to library patrons. It must be mentioned that efficiency has been always the desire of library professionals throughout the world in their attempt to provide improved service to library patrons.

5.3 Effectiveness of the Security Systems put in place in Libraries of Higher Institutions of learning understudy

The study sought to know the effectiveness of the inscription of library materials which was used as a security measure on print and other materials like furniture. The study revealed that the inscription measure was effective. This is because security guards and library staff have intercepted a lot library material that were meant to be stolen by library users. This was facilited with the use of secrete page numbers. A secrete page make it easier for security guards at the checkpoint to intercept those who try to steal library materials. However, few libraries were of the view that the security measures were not effective. This is because thieves managed to steal materials. These libraries lost their materials because thieves managed to see and remove the inscribed words or pages with security features. When inscription is removed security guards find it difficult to identify library materials.

The findings further revealed that a lot of libraries were of the view that the cloakroom was not effective. This is because library users have continued losing their items. Poor implementation of security systems and lack of good maintenance of the cameras led to loss of user's belongings. The libraries continued losing items due to lack of physical security to man the cloakroom. Therefore, there is a need for libraries to employ enough security personnel to be taking care of user's belongings at the cloakroom as this will stop patrons from serving themselves. The deployement of ecurity officers at the cloakroom can minimize theft. However, few libraries indicated that the security measure was quite effective because libraries rarely received complaints from library users having lost their items from the cloakroom or locker/cabinet. The reason leading to this is because security officers or library staff are in charge of the cloakroom and they have made sure that no library user is allowed to get an item without the help of the security. When users are allowed to get their belongings on their own this can promote theft at the cloakroom. It is very important that this place is manned by a security guard all the time if items for readers are to be safe.

Respondents from a lot of libraries indicated that fire extinguishers in their libraries were not effective because they were not serviced from the time they were installed. This came about due to lack of funds for servicing. The other reason is that library management have not realized that fire extinguishers are suppose to be serviced regulary. The problem with this is that if fire break out the gadget will not be able to function and library materials can catch fire. For these extinguishers to be effective there is a need for maintenance and servicing to be done frequently of which all libraries must strive to do. There is also a need for library staff to know at least the

basics of how to use the fire system and this can be done by having the staff trained. However, few libraries were of the view that their gadgets were effective. The reason is because they have managed to quench fire before and this was achieved due to regularly maintenance. This is a sign that these institutions allocate funds and acknowledge the importance of maintaining fire extinguishers, so that they can perform effectively at any given time. Therefore, libraries should always strive to service their fire extinguishers for the betterment of protecting library resources.

The study further established that a lot of libraries were of the view that charging penalty fee for books brought late was effective because several library books were returned after its introduction. This proves to be a useful because patrons cannot afford to give out their money when they can return books on time. It was also reviewed that amnesty week was effective because several books were returned during this week. The reason is that during amnesty week all those who were keeping overdue materials were encouraged to bring them back without paying a penalty fee regardless of the period they have kept them. This really motivated library users to return overdue books**.** However,few respondents were of the view that the security measure was not effective because some books were not returned after its introduction. The measure proved not to be effective because of poor publicity by library management. Therefore, library managers should be urged to sensitize users about this week if it is to be effective.

Respondents from a lot of libraries were of the view that security guards were effective in protecting library resources from theft. This is because there has been massive reduction in theft of library materials due to the presence of security guards which instill fear to library users. Another reason is that these libraries have enough officers such that they do not leave their stations unmanned and they are also able to carry out routine patrols. The other reason is that these security guards were trained and orientated properly on how to identify library materials from personal items. It should be taken into consideration that physical security has an upper hand as compared to the electronic system. This is because officers can check effectively for library materials even when there is no power through the use of other sources of lighting like lamps. Electronic security systems become nonfunctional when there is power outage. Therefore, libraries must employ officers to be working hand in hand with other security systems.

However, the findings from few libraries revealed that security guards were not effective because they have continued losing their materials with their presence. The reason for having

continued experiencing theft in these libraries is that the security personnel are understaffed hence unable to take patrols. At times officers also leave critical areas unattended to and the moment they leave the station thieves take this as an opportunity to steal. Libraries should ensure that they have enough manpower to undertake the necessary duties. The other reason is that users at times connive with security officers or corrupt them so that they allowed them to pass with stolen books. To avoid this there is a need for security officers to be paid well and provide conducive working environment to them because what makes them accept to be bribed is hunger.

The study further established that closed circuit television cameras installed in a lot of libraries were effective. This is because theft of library materials reduced drastically after their installation. Thieves were also captured in the camera trying to steal and were intercepted. The effectiveness of these cameras was as a result of regular maintenance and serving of the devices. Another factor that led to this was because the security guards or library staff in the monitoring room have been always available to watch the activities going on in the library. The presence of cameras can also play a significant role in the sense that even when cameras are not functioning users are restrained from stealing and this can reduce crime. The findings of this study were in agreement with Osayande (2011), who indicated the effectiveness of cameras. The surveillance detection system is effective if installed properly and can be used as a tool to effectively prevent library items from leaving the library.

However, few libraries indicated that the devices in their libraries were not effective. The reason is that these libraries have continued losing their resources. This was caused by a lack of regular maintenance of the security systems and this is a security threat to library resources. When cameras are not regularly serviced they become ineffective and because of this a library can continue missing its resources. At times cameras can be effective but if there is no one in the surveillance control room to monitor what is happening a library can continue losing materials. Another problem is that some libraries installed cameras only on few selected sections of the library. The danger of not installing cameras in all areas of the library is that it poses security threats to library materials. This becomes a problem when users realize that some areas are not installed with camera and they can use such places to abuse the materials. Library administrators should make sure that CCTV cameras are maintained regularly for them to be effective and they should be placed in all areas of the library. The closed-circuit television room must always be manned so that those doing wrong things do not scot-free.

The findings further indicated that the 3M book detection systems in few libraries were effective. This is because there was book theft reduction after the installation of the device and a number of library users were intercepted at the exit try to smuggle some books. The availability of funds and expertise for regular maintenance and servicing made the devices to be effective. Furthermore, the loud sound that the device produce restrain patrons from stealing. The embarrassment they would go through when it produces the sound that everyone can hear in the library is another restraining factor. The results of the study is in line with Ali (2016), who also suggests the use of electromagnetic systems to combat theft of library materials.

However, the 3M detection systems installed in some libraries were not effective. The reason is due to poor maintaince and lack of expertise to look after the gadgets. This is because of insufficient funds which most libraries are facing. Library management must make sure that the devices are serviced so that the whole essence of acquiring the device is not defeated after spending huge sums of money on them.

The results further showed that alarm systems installed in few libraries were very effective because theft of materials drastically reduced. This is due to the fact that every time thieves tempered with windows or doors the alarm system produced an audible sound and this scared away intruders. Sensors must be placed in all the windows and doors of the library as this will ensure that there is no weak point. These libraries also managed to prevented intruders from illegally entering the library by ensuring that their gadgets are always left activated when libraries close down for the day.

However, the alarm systems installed in few libraries were not effective because thieves have managed to break in and store library materials. The alarm systems installed in these libraries wer not maintained or serviced regularly due to inadeguate funding allocated to libraries. Another reason is due to lack of staff with skills to maintain and repair the device. This is beacuse whenever the gadget has a small problem these libraries have to engage experts from outside the country which is expensive. To resolve this problem there is need to train people from within the institution on how to install and maintain the gadget. That way it becomes cheaper and quicker to service the security device rather than depending on experts from outside the institution or country at large**.**

The study further revealed that smoke detectors were quite effective as they have detected smoke before immediately when fire started. This was facilitated by good maintenance practices and the devices have been placed in strategic points for them to be able to detect

smoke. For this equipment to be effective, it must be connected to a central panel of which must be connected to the fire department so that firefighters can easily be notified. There is as well need to install smoke detectors in all hallways of the building so that smoke can quickly be detected.

The findings further showed that the radio frequency identification installed is effective because it has reduced theft of print material and it has improved service delivery. The findings are in line with Rathinasabapathy and Rajendran (2015) who highlighted the effectiveness of radio frequency identification (RFID) systems when handling security of the library collection. This device has been effective because it has managed to control access to the library to those who did not have cards and the device has tracked many stolen books. What has contributed to its effectiveness is due to regular maintenance and servicing which has improved its performance. Management must always know that good maintenance and servicing do not happen by accident but requires careful planning and proactive management.

5.4 Summary of Chapter Five

This chapter presents the discussion and interpretation of the results of the research. The chapter also integrated the results in chapter four which discussed the findings of the study with information from other studies done from the literature used in this study.

It is evident form the findings that libraries of higher education institutions face different types of security problems in Zambia which comprise theft, vandalism and mutilation of library materials. The study revealed a number of methods were used by library users to steal materials such as hiding materials in clothing, pushing materials through windows, smuggling books in bags and through impersonation. Library users were able to abuse library materials because in some of the libraries monitor rooms for surveillance cameras were left unattended. In a normal situation libraries are supposed to have mesh wire on their windows so that theft of library materials is stop. It has come to the attention of the researcher that some libraries do not have protective measures like mesh wire on the windows.

The study further highlighted that libraries were also facing computer related security issues like theft, computer viruses, password sharing and deletion of data. In order to minimize threats to computer equipment and computer-based information system. These libraries have not just sit back and watch but they have tried to put in place some preventive measures. The use of passwords to protect vital information shows how committed libraries are in terms of protecting

the information. Above all institutions have also acquired backup systems, USPs and staff have been trained that no data is lost.

The findings further revealed that a lot of libraries had problems with power outages particularly in the night did not secure generators to prevent theft of library resources. The installation of generators is quite important as it does not only protect library resources from being stolen, but also to ensure that services are delivered as required. However, some libraries have installed standby generator due to among other reasons, awareness of the consequences that comes with power outage. These problems pose serious challenges to libraries in terms of service provision. The findings have shown that libraries are not funded adequately which makes them to have less purchasing power to acquire necessary security systems.

It is clear from the findings that libraries have managed to acquire security systems although they have problems to maintain them and a number of these devices were not working due to lack of regular maintenance. The effect of losing print materials is that it becomes a drawback replacing lost materials because this money can be used for other developmental issues. The other effect is that library users are denied an opportunity to have access to materials when they want conduct their research.

According to the results of the study, libraries have put in place some security measures to mitigate security problems libraries encounter such as the installation of CCTV cameras, 3M book detection system, alarm systems, fire extinguishers, smoke detectors and the provision of security guards. Furthermore, in terms of the effectiveness of the security systems used by libraries of higher institutions of learning under study. The findings of the study indicate that a lot of the respondents were of the view that most of the measures were effective.

In this chapter some challenges were identified in ensuring security in the libraries and some the challenges include inadequate funding, incompetent staff and poor maintenance of ICT infrastructure. The most prominent one is that a lot of libraries did not receive adequate funding for security systems from top management. Insufficient funding makes it difficult for libraries to implement stringent measures to acquire and secure library resources. This problem have been in existence because libraries have failed to come up with policies which guide on how to protect the already acquired library materials. A policies is necessary in the library because it has the ability to ensure that library administrators and top management comply with the guidelines on how to secure funds for purchasing and maintenance of the security systems.

CHAPTER SIX: CONCLUSION AND RECOMMENDATIONS

6.0 Overview

The main objective of this study was to investigate security problems and measures put in place to prevent theft of library resources in selected academic libraries in Zambia. The study also sought to dertimine the types of security problems being faced by libraries of higher education institutions in Zambia; dertimine security measures libraries higher education institutions have put in place to mitigate against security problems libraries are facing; establish the effectiveness of the security systems used by academic libraries under study. Therefore, it is from this background that the chapter intends to make conclusions and recommendations of the study.

6.1 Conclusion

The chapter presents the establishment of the research findings. The security of print and non-print materials is crucial to the librarians in order to reduce unauthorised people from accessing the resources.The findings of this study revealed that numerous security problems were being faced by libraries of higher learning institutions in Zambia included theft and mutilation of library materials power cuts, vandalism, and unauthorised access to library materials. Library management should come up with measures or strategies that will help them to provide adequate security, help to protect, and make sure resources are available as this will fulfill library goals of meeting the information needs of users. However, the use of security systems requires management support in terms of funds, staff support for the attainment of the set goals. Therefore, there is a need for library management to release the funds that are needed for the accomplishment of the task.The benefits of using security systems in libraries of higher institutions of learning cannot be ignored because of the important role that they play in providing security to library resources. Libraries of higher education institutions need effective security measures that can protect their materials since they are expected to give quality information to their users.

It must be noted that the importance and usefulness of security systems or devices in libraries is to help provide maximum and adequate security for library resources, employees, patrons, and the entire library building. It is necessary for these security systems or devices made available in libraries. The usefulness of these security measures cannot be overemphasized because of the following benefits: prevention of theft in the library, flexibility, remote monitering, maximum security to the library buildings and resources.

According to the study, some of the security measures libraries have put in place to mitigate against security problems encountered were the use of security guards, installation of CCTV cameras, fire extinguishers, use of inscription of library materials, use of 3M book detecting system, alarm systems, smoke detectors, use of clock rooms and provision of security guards. The findings reviewed that although some libraries have installed electronic security systems their security systems were not working because of lack of maintenance and servicing. The study further revealed that a lot of respondents indicated that the security systems installed in their libraries were very effective.

6.2 Recommendations

Having the challenges established, some recommendtion have been proposed which include:

(i) Proposing to have all librarians oriented in security-related issues so that they can handle any security threat to library materials. Library staff must understand all kinds of security threats that libraries are exposed to and also how to mitigate them.

(ii) Management should ensure that sufficient funds are allocated to libraries; this will help in bringing the needed security systems

(iii) Libraries in Zambia should install Closed Circuit Television (CCTV) cameras to trengthen the security system.

(iv) Higher learning institution should acquire standby generators to use in case of power outages. Generators would surely mitigate the power outage in libraries that have not yet installed them. This would in return stop disruption of library operations and ensure continuity of library services.

(v) Libraries should develop a policy on security management teams that will be working hand in hand all the time with security guards.

(vi) Libraries of higher education institutions of learning in Zambia should have a written policy that covers security measures that will help other new staff and the academic community to know what is on the ground for them to follow strictly.

(vii) All libraries in higher learning institutions should procure fire extinguishers and train library employees on how to use them.

(viii) The researcher recommends that further study should be conducted which will look at the role librarians should place to enhance security of library resources.

REFERENCE

Abioye, A. & Adeow, O. F. (2013). "Security Risks Management in Selected Academic Libraries in Osun State, Nigeria." *The Information Manager*, 3, (2), 1-9. file:///C:/Users/Hp/Downloads/106874-Article%20Text-290877-1-10-20140822%20(2).pdf

Abioye, A. A. & Rasaki, O. E. (2013). "Survey of Security Challenges in University Libraries in Southwest Nigeria." *Library & Archival Security*, 26 (1-2), 1-13. DOI:10.1080/01960075.2013.869078

Abubakar.F & Aduku.B.S (2016). ''Approaches to Security of Information Resources in Academic Libraries in Niger State, Nigeria.'' *Samaru Journal of Information Studies*, 16(1), 12-24. https://www.ajol.info/index.php/sjis/article/view/174811

Abu-Musa, A. (2010). "Information security governance in saudi organizations: an empirical study." *Inf. Manag. Comput. Secur*. 18 (4), 226–276. doi:10.1108/ 09685221011079180.

Adebayo J.O & Adekunjo OA. (2013). "The challenges in the development of an academic digital library in Nigeria." *International Journal of educational research and Development*; 2(6), 152-157. http://academeresearchjournals.org/journal/ijerd

Adekunle, F.A., Adekunjo, O.A., and Unuabor, S.O (2018). ''Theft and Vandalism: Effect and Control Mechanism on Information Resources in Academic Libraries in Osun State, Nigeria.'' *IOSR Journal of Humanities and Social Science (IOSR-JHSS)*, 23 (7), 71-78

Adewuyi, O.W. & Adekanye, E. A. (2011). "Strategy for prevention of crime in Nigerian University libraries: The experience of the University of Lagos."*Library and Archival Security* 24(1),25-37. Retrieved from http://www.tandf.co.uk /journals/tittles/01960075.asp

Agyen. G, K. (2008). "User education at the Kwame Nkrumah University of Science and Technology (KNUST): prospects and challenges." *Library Philosophy and Practice,Annual Volume."*Available at: http://unllib.unl.edu/LPP/agyen-gyasi.htm

Ahenkorah-Marfo, M. & Edward M. B. (2010), "Disaster preparedness in academic libraries: the case of the Kwame Nkrumah University of science and technology library, Kumasi,Ghana."*Library&ArchivalSecurity*,23(2),117-136. https://www.tandfonline.com/doi/full/10.1080/01960075.2010.501417

Ajegbomogun, F.O. (2004). "Users' assessment of library security: a Nigerian university case study." *LibraryManagement*, 25 (8/9) 86-390. https://doi.org/10.1108/01435120410562880

Akor, P. U. (2013). "Security management for prevention of book thefts in university libraries: A case study of Benue state university library, Nigeria." *Library Philosophy and Practice(e-journal).* Paper 995. http://digitalcommons.unl.edu/libphilprac/995. (Accessed May 2, 2019)

Akussah, H. & Bentil W. (2010). “Abuse of library materials in academic libraries: A study of the University of Cape Coast main library.” *African Journal on Librarianship, Archival and Information Science*, 20 (2), 103-112. http://197.255.68.203/handle/123456789/1250

ALA (2009).“The condition of US libraries: academic library trends, 1999-2009.” https://www.ala.org/tools/sites/ala.org.tools/files/content/librarystats/librarymediacenter/Condition_of_Libraries_1999.20.pdf (Accessed October 2018).

Alao, I.A, Folorunso, A.L & Saka, H.T. (2007). Book availability in the University of Ilorin College of Health Sciences Library. *World Libraries*, 17 (2), 14-24. https://worldlibraries.dom.edu/index.php/worldlib/article/view/35/60

Alavi, R., Islam, S & Mouratidis, H. (2016). “An information security risk-driven investment model for analysing human factors.” *Inf. Comput. Secur*. 24 (2), 205–227. doi:10.1108/ICS-01-2016-0006.

Ali, M.Y. (2016).’’ Library book theft and audits in university libraries of Pakistan.*” Journal of Library Administration*, 57(1), 87-98. https://doi.org/10.1080/01930826.2016.1251252

AlHogail, A. (2015). “Design and validation of information security culture framework.” Comput. *Human Behav*. 49, 567–575. doi:10.1016/j.chb.2015.03.054

Allen, J. & Westby, J.R. (2007). Characteristics of effective security governance. Governing for Enterprise Security (GES) Implementation Guide (CMU/SEI-2007-TN-020). Software Engineering.

Al-Suqri. M. & Afzal W. (2007). “Digital age: Challenges for libraries.” *Information, Society and Justice*, 1(1), 43-48. doi: 10.3734/isj.2007.1105.

Ameen, K. & Haider, S.J. (2007).“Evolving paradigm and challenges of collection management in University libraries of Pakistan*.” Collection Building*, 26 (2), 54-58. DOI:10.1108/01604950710742086

Amini, M. Vakilimofrad, H. & Saberi, M.K. (2021), "Human factors affecting information security in libraries", *The Bottom Line*, 34 (1), 45-67. https://doi.org/10.1108/BL-04-2020-0029

Ashenden, D. (2008). “Information security management: a human challenge*?” Infor. Secur. Tech. Rep.* 13 (4), 195–201. doi:10.1016/j.istr.2008.10.006

Anderson, K. (2007).” Convergence: A holistic approach to risk management.” *Network Security*, 5: 4-7. https://doi.org/10.1016/S1353-4858(07)70033-8

Ansari, A. J. & Ali, P.M. N, (2021). "Security Challenges in Central University Libraries in India". *Library Philosophy and Practice* (e-journal). 5299. https://digitalcommons.unl.edu/libphilprac/5299

Aravind, S. (2019). "college librarian satisfaction of library security system-a study." *INFOKARA RESEARCH*, 8 (9), 801-808. http://infokara.com/gallery/100-sep-2977.pdf

Association of College & Research Libraries. RBMS Security Committee (2006). Guidelines for the security of rare books, manuscripts and other special collections. ‘*’C & RL News, Jul/Aug’’*: 426-433. Available at: http://www.ala.org/ala/mgrps/divs/acrl/standards/securityrarebooks.cfm

Ayoung, D.A. Boatbil, S.C. & Sanbil, S. (2014). How secure are library collections? an evaluation of polytechnic libraries in Ghana. Information and Knowledge Management. 4 (3), 56-66. Retrieved from www.iiste.org

Azerikatoa. D. A. Christopher S. B & Sadat. B (2014). How Secure are Library Collections? An Evaluation of Polytechnic Libraries in Ghana. *Information and Knowledge Management*, 4(3), 56-66. file:///C:/Users/Hp/Downloads/Paper3%20(1).pdf

Aziagola, P. C. & Edet, G. T. (2008). Disaster-control planning for academic libraries in West Africa. *The Journal of Academic Librarianship*, 34 (3), 265-268. DOI10.1016/j.acalib.2008.03.011

Baba, M.K. & Tripuram, V.R.(2014). “Implementation RFID technology for library security: A proposal of Maulana Azad National Urdu University (MANUU*)”, International Journal of Innovative Research and Developmen*t, 3 (12), 151-157. https://www.ijird.com>article>view

Balas, J. (2005).“Close the gate, lock the windows, bolt the doors: Securing library computers.” *Computers in Libraries*, 25 (3), 28-31. https://eric.ed.gov/?id=EJ684017

Basaka A**.** A et al (2020). ‘’Security Challenges and Control Measure in Four Academic Libraries in North East Nigeria University Libraries.’’ *Journal of science technology and education*, www.atbuftejoste.com

Baskerville, R. L et al (2005). "Information Systems Security Standards: The Solution or the Problem?" *ECIS 2005 Proceedings*. 159. http://aisel.aisnet.org/ecis2005/159

Bhande, A.P.(2014). "Use of Security Tools in Libraries: An Innovative Perspective." Dnyanobarao,S. &Veer, D.K.(Eds), Digital Libraries, E-Resources, and E-Publishing, Ess Ess Publications, New Delhi, pp.440-446.

Berthelot, S. (2013). “How to Inventory a Church Library Collection. *LifeWay Christian Resources*.” [Online] Available: http://www.lifeway.com/Article/Church- ‘ library ministry-inventory-process-for-a-librarycollection

Brown, K. E., & Parkus, B. L. (2007). Collections security: planning and prevention for libraries and archives. Retrieved from http://www.nedcc.org/resources/introduction.php

Buecker. A (2010). Introducing the IBM Security Framework and IBM Security Blueprint to

Realize Business-Driven Security. *IBM RedGuide, New York.* Available at: http://www.redbooks.ibm.com/redpapers/pdfs/redp4528.pdf.

Campbell, J. D. (2006).“Changing a cultural icon: the academic library as a virtual destination.” *Educause Review,* 41 (1) 16–31. https://er.educause.edu/-/media/files/article-downloads/erm0610.pdf

Carey, J. (2008). “Library security by design.” *Library and Archival Security*, 21(2). Retrieved from www.haworthpress.com

Casson, L. (2001). ‘’Libraries in the Ancient World. London: Yale University Press.

Castro, J (2008). “Data protection: where are we now?” *Journal of Database Marketing and Customer Strategy Management,* 15 (4), 285-92

Chaputula, A. & Boadi, B.Y. (2010). “Funding for collection development activities at Chancellor College Library, University of Malawi.” *Collection Building*, 29 (4), 142-7, available at: DOI 10.1108/01604951011088871] (accessed 13 March 2019).

Chatterjee, A. & Maity,A.(2013). "Security Challenges in University Libraries of India." *Thanuskodi,S.(Ed), Challenges of Academic Library Management in Developing Countries, IGI Global*, pp. 94-111. DOI:10.4018/978-1-4666-4070-2.ch008

Chen, Z., Wei, P. & Delis, A. (2008). “Catching Remote Administration Trojans (RATs).” *Software, Practice & Experience,* 38 (7), 667-703. https://doi.org/10.1002/spe.837

Chiemeke, S, et al (2007). “Users' perceptions of the use of academic libraries and online facilities for research purposes in Nigeria.” *Library Philosophy and Practice.* Available at: https://digitalcommons.unl.edu/libphilprac/116 . (Accessed January 11, 2020).

Chifwepa, V. (2006). Development of a model plan for the application of information communication technologies in Distance education at the University of Zambia. PhD thesis. University of Zambia

Chinwendu.N. A (2019)."effect of theft and mutilation on the use of library collection in an academic library in lagos state." *Library Philosophy and Practice (e-journal*). 2548. https://digitalcommons.unl.edu/libphilprac/2548

CLUSIF. (2008). Information Systems Threats and Security Practices in France. Available at: https://www.clusif.asso.fr/fr/production/sinistralite/docs/CLUSIF- . apport-2008- en.pdf

Connaway, L. S. & Powel, R. R. (2010). Basic Research Methods for Librarians. Santa Barbara, CA: Libraries Limited.

Chow, W. S & Ha, W. O. (2009). “Determinants of the critical success factors of disaster recovery planning for information Systems*.” International Management & Computer Security,* 17 (3), 248-275.

https://doi.org/10.1108/09685220910978103

Cowan, J. (2003). ‘’Risk management, records and gaming report.’’ *Clinical Governance: an International Journal*, 8 (3), 275-277. http://hdl.handle.net/10760/18215

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

Da Veiga. A & Eloff. J.H.P (2007). ‘’An Information Security Governance Framework.’’ *Information Systems Management*, 24 (4), 361-372, DOI: 10.1080/10580530701586136

Dawe, M. (2017). Electronic Security Systems: Technical Specification & Design Guidance Document. London: UCL.

Doherty, N.F & Fulford, H (2006). “Aligning the information security policy with the strategic information systems plan.” *Computers & Security*, 25 (1), 55-63 https://doi.org/10.1016/j.cose.2005.09.009

Eisenberg. J & Lawthers, C. (2008). “Library Computer and Network Security: Library Security Principles.” *Infopeople Project*. Available at: http://www.infopeople.org/resources/security/basics/index.html.

Engebretson, P. (2011). The basics of hacking and penetration testing, Boston: Syngress

Etsebeth, V. (2007). “Malware: the new legal risk.” *The Electronic Library*, 25 (5) 534-552.https://doi.org/10.1108/02640470710829523

Ezeabasili, C. A (2018). "Use of Electronic Security Systems in the Security of Information Resources in Federal University Libraries in Southern Nigeria". *Library Philosophy and Practice (e-journal*). 2109. http://digitalcommons.unl.edu/libphilprac/2109

Ezeabasili, C. A, (2018). "Impact of Electronic Security Systems in the Security of Information Resources in Federal University Libraries in Southern Nigeria." *Library Philosophy and Practice (e-journal).* 2110. http://digitalcommons.unl.edu/libphilprac/2110

Farahmand, F, et al (2005). “Assessing Damages of Information Security Incidents and electing Control Measures, a Case Study Approach.” *Workshop on the Economics of Information Security*, available at: http://infosecon.net/workshop/pdf/39. (Accessed August 5, 2018.

Fasae, J. K. & Adedokun, F.O. (2016), "Abuse of Information Materials in Academic Libraries by Students of Tertiary Institutions in Ekiti-State, Nigeria." *Library Philosophy and Practice.* https://www.researchgate.net/publication/309720065

Fox, E. & ElSherbiny, N. (2011). Security and digital libraries, digital libraries - methods and applications, Kuo Hung Huang (Ed.), InTech, Retrieved on April 2019 from http://www.intechopen.com/articles/show/title/security-and-digital-libraries

Fullard, A. (2007). “South African responses to open access publishing: a survey of the research community.” *South African Journal of Libraries and Information Science*, 73 (1), 40-50. http://hdl.handle.net/10566/30

Gautam, V., Behera, P. K. & Singh. M (2011). ‘’Issues of digital data security in the library environment.’’ *International Journal of Information Dissemination and Technology*, 1(4), 127-140.

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

Green, J. & Thorogood, N. (2009). Qualitative Methods for Health Research (Introducing Qualitative Methods series) 3rd edition. Paperback – 1601. Retrieved fromhttp://www.amazon.com/Qualitative-Research-Introducing-ThorogoodPaper back/

Griffiths, R & Krol, A. (2009). “Insider Theft Reviews and Recommendations from the Archive and Library Professional Literature.” *Library and Archival Security*, 22 (1), 5-18. DOI:10.1080/01960070802562834

Guel, M.D. (2007). A Short Primer for Developing Security Policies. Available at: http://www.sans.org/resources/ policies/Policy_Primer.pdf

Gupta, M & Sharman, R (2008). Social and Human Elements of Information Security: Emerging Trends and Countermeasures. Hershey: PA, IGI Global.

Hadow, K. (2009). “Data security for libraries: Prevent problems, don’t detect them.” *Feliciter*,55(2),22-46.http://www.ajindex.com/dosyalar/makale/acarindex-1423872811.pdf

Hagen, J.M., Albrechtsen, E. & Hovden, J (2008). ‘’Implementation and effectiveness of organizational Information security measures.’’*Information Management & Computer Security*, 16 (4), 377-397. https://doi.org/10.1108/09685220810908796

Haglund, L, & Olsson, P. (2008). “The Impact on university libraries of changes in information behavior among academic researchers: a multiple case study.” *The Journal of Academic Librarianship*, 34 (1) 52-59. DOI:10.1016/J.ACALIB.2007.11.010

Halubanza. B, Kunda.D & Musonda.Y (2021).‘’An assessment of Information Security Awareness among employees in Higher Education Sector in Zambia: A case of Zambia’s public Universities’’. 1-14, Available at: https://space.mu.ac.zm/xmlui/handle/123456789/186

Haniza S. (2009). Users' perception of the information security policy at the University Teknologi Malaysia. Master’s thesis, University Teknologi Malaysia, Faculty of Computer Science and Information System. Available at: http://eprints.utm.my/id/eprint/5291/

Hariyanto.A & Siahaan.A.P (2016) "Intrusion Detection System in Network Forensic

Analysis and Investigation." *IOSR Journal of Computer Engineering*, 18 (6), 115-121.DOI:10.9790/0661-180604115121

Hassanain, M.A. and Al Ashwal, N. (2005), "An approach to assess fire safety requirements in library facilities", *Facilities*, 23 (5/6), 239-252. https://doi.org/10.1108/02632770510588646

Hedström, K, et al (2011). "Value conflicts for information security management." *Strateg. Inf. Syst.* 20 (4), 373–384. doi:10.1016/ j.jsis.2011.06.001.

Henrich, K. J. & Richard A. S. (2016). "Library safety through design: using a checklist approach at the University of Idaho." *Journal of Library Administration*, 56 (7), 777-789. DOI:10.1080/01930826.2015.1124705

Holt, G. E. (2007). "Theft by library staff." *The Bottom Line Managing Library Finances*, 20(2): 85-93. https://doi.org/10.1108/08880450710773020

Hu, Q, et al (2012). "Managing employee compliance with information security policies: the critical role of top management and organizational culture." *Decis. Sci*.,43 (4), 615–660. doi:10.1111/j.1540-5915.2012.00361.x

Ibraheem, A.I. & Devine, C. (2013). "Brain drain in African academic libraries: a Survey." *Library Review*, 35 (6/7), 13-31. https://doi.org/10.1108/LR-10-2012-0113

Idris, M., Hassan, U. & Abdul-Qadir**,** F. (2013) "Theft and mutilation of library materials in academic libraries: The case study of Kano University of science and technology, Wudil, Kano State, Nigeria." *Journal of Research in Education and Society*, 4(3), 44-55.

Isebe, I.E.M. (2014). "Cause and effects of theft and mutilation of information materials in academic library services in delta state." *Journal of Information Knowledge and Management.* 4(10), 76-82. Available at: https://core.ac.uk/download/pdf/234671825.pdf

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

Jagadish, M. V. & Sarasvathy.P (2018). "What Librarians Think of Theft, Mutilation, and Misplacement of Library Resources? A Study of Karnataka University Libraries". *Journal of Advancements in Library Sciences*, 3 (3), 7-14. http://irjlis.com/wp-content/uploads/2017/02/15-IR-366-64.pdf

Karin, d. J. (2018). ''The use of academic libraries in turbulent times: Student library behaviour and academic performance at the University of Cape Town.'' *Performance Measurement and Metrics,* 19 (1), 40-52. Available at: https://doi.org/10.1108/PMM- 09-2017- 0037

Kaur, T (2009). "Disaster planning in University Libraries in India: a neglected area." *New Library World*, 110, (3/4), 175-187. https://doi.org/10.1108/03074800910941365

Kimwele, M., Mwangi, W & Kimani. S (2005). ‘’Adoption of Information Technology Security Policies: Case Study of Kenyan Small and Medium Enterprises.’’ *Journal of Theoretical and Applied Information Technology*, 18(2), 1-12.

Knapp, E.D. & Samani, R. (2013). Applied security and the Smart Grid: Implementing security controls into Modern power infrastructure, London: Elsevier

Knapp,K.J, et al (2009).” Information security policy: an organizational-level process model.” *Comput. Secur*. 28 (7), 493–508. doi:10.1016/j.cose.2009.07.001

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

Kraemer, S., Carayon, P. &Clem, J (2009). “Human and organizational factors in computer and information security: pathways to vulnerabilities.” *Comput. Secur*. 28 (7), 509–520.doi:10.1016/j.cose.2009.04.006

Kruger, I., Nickolay. B. & Gaycken, S. (2013). The secure of Information, London: Springer

Kumar, N. (2014). Library Security Through Networking of CCTV Surveillance: A Study of Sikkim University, Sikkim." 9th Convention PLANNER-2014 Dibrugarh University, Assam, September 25-27, 2019. http://hdl.handle.net/1944/1798

Kumbhar, K.N, & Veer, D.K (2016). "Study of Vulnerable and Delinquent Activities in College Libraries." *Journal of Advances in Library and Information Sciences*, 53 (1), 52-59.http://jalis.in/pdf/5-1/Kumbhar.pdf

Kawulich, B.B. (2005). Participant Observation as a Data Collection Method. Forum: Qualitative Social Research.6,2, Art. 43. Retrieved from http://www.qualitative-research.net/index.php/fqs/article/view/466/996.

Kuzma, J. (2010). “European digital libraries: Web security vulnerabilities.” *Library Hi Tech*, 28(3), 402-413. doi: 10.1108/07378831011076657

Lavanya.p (2017). ‘’Security Systems in Libraries: An overview.’’ *International Journal of Library and Information Studies,* 7(1). *http://www.ijlis.org*

Lucky, O.U., Daniel, E. & Joy, E.O. (2018).“Security measures were adopted to prevent theft of library resources in selected academic libraries.” *International Journal of Library and Information Science Studies*, 4 (1), 1-10.

Maidabino, A. A. & Zainab, F. (2011**).** Collection security issues in Malaysian academic libraries: An Exploratory Survey file:///C:/Users/Hp/Downloads/maidabino_ngah%20(16).htm

Maidabino, A.A. (2012). “Theft and mutilation of print collection in university libraries: A critical review of literature and proposed framework for action.*’’Annals of Library and Information Studies* 59,(2) 240-246. http://op.niscair.res.in/index.php/ALIS/article/download/162/26

Maidabino,A.A (2011). “Collection security management at university libraries: assessment of its implementation status.“*Malaysian Journal of Library & Information Science*.”

16(1). http://myais.fsktm.um.edu.my/11640/1/no._2.pdf

Mansfield, D. (2009). "Reducing book theft at university libraries." *Journal of Library and Information Research,* 33(103), 10- 15. DOI:10.29173/lirg98

Marcus, I. L.E. (2014). "Cause, and Effects of Theft and Mutilation of Information Material in Academic Library Services in Delta State." *Information and Knowledge Management*, 4, (10), 76-82.https://core.ac.uk/download/pdf/234671825.pdf

Matthew. G (2004). Preservation and management: Sources of information. In John Feather (Ed.), Managing preservation for libraries and archives: Current practice and future developments, 153-154). Burlington: Ashgate Publishing

McKay, A. & Yakel, G. (2006). "ARCHIVES AND MANUSCRIPTS Copyright news: Orphan Works and Section 108: reproduction by libraries and archives OCLC Systems & Services*." International digital library perspectives*, 22(4), 241-246. Available at: www.emeraldinsight.com/1065-075X.htm (Accessed September 26, 2018).

Merete, H. J., Albrechtsen, E. & Hovden, J. (2008)."Implementation and effectiveness of organizational information security measures." *Inf. Manag. Comput. Secur*., 16 (4), 377–397.doi:10.1108/09685220810908796

Momodu, M.A. (2002). ''Delinquent readership in selected urban libraries in Nigeria.'' *Library Review* 51 (9): 469-473.

Moyo, L.M. 2004. Electronic libraries and the emergence of new service paradigms. *The Electronic Library*, 22(3) 220-230: https://doi.org/10.1108/02640470410541615

Munir.A, et al (2012). Human Errors in Information Security. International Journal of Advanced Trends in Computer Science and Engineering, 1(3), 82-85. Available at http://warse.org/pdfs/ijatcse01132012.pdf

Nathans, D. (2016). Designing and building a security operations center, London: Elsevier.

Nielsen, E. (2002). Library security management: An introduction. *Liber Quarterly*, 12 (5), 293-295.

Odaro.O (2019). Use of electronic security systems in academic libraries: experiences of selected universities in south-west Nigeria: unpublished: Available at: https://ukzn-dspace.ukzn.ac.za/bitstream/handle/10413/17712/Odaro-Osayande-2019.pdf?sequence=1&isAllowed=y

Ogbonyomi, A. L. (2011). "Security and Crime Prevention in Academic Libraries: A Case Study of the Kano State College of Education, Kano, Nigeria". *Library Philosophy and Practice (e- journal)*. 496. https://digitalcommons.unl.edu/libphilprac/496

Oghenetega.L .U, Emojorho. D & Omah.J.E (2018). Security measures adopted to prevent theft of library resources in selected academic libraries in nigeria, 4, (4), 42-51. https://www.eajournals.org/wp-content/uploads/Security-Measures-adopted-to-

Prevent-Theft-of-Library-Resources-in-Selected-Academic-Libraries-in-Nigeria.pdf

Ogunsola, L. A. (2006) “Nigerian University Libraries and the Challenges of Globalization: The Way Forward." *E-JASL 1999-2009*, 43 (1-10). https://digitalcommons.unl.edu/ejasljournal/43

Ogunyade, T.O. (2005). ‘’Theft and Mutilation in an Academic Library.’’ *College of Medicine, University of Lagos Experienc*e, *Nigot, J, Hosp. Med*.,15(2),13-19. (available at:http//:www.unilag.edu.ng, (accessed May 25, 2018).

Olajide, O.(2017), "Theft and Mutilation Challenges and Management in Academic Libraries: A Case Study of Federal University Oye-Ekiti, Nigeria." *Journal of Applied Information Science and Technology*, 10 (1). https://www.jaistonline.org/10vol1/JAIST%20PAPER%2010%20 Theft%20and%20Mutilatio n%20Challenges%20recent.pdf

Olayemi, O.A. (2005). University of East London School of Computing and Technology, System Integration, CNM009. http://homepages.uel.ac.uk/u0430614/classification of security threa.htm.

Olugbenga. W. A & Elizabeth A. A (2011). ‘’Strategy for Prevention of Crime in Nigerian University Libraries: The Experience of the University of Lagos. *Library & Archival Security*, 24 (1), 25-37. https://doi.org/10.1080/01960075.2011.552315

Omoike. A & Alabi. R (2020). ’’Theft, Mutilation and Abuse of Library and Information Materials by Undergraduates of University of Ibadan, Nigeria.’’ *Information Impact: Journal of Information and Knowledge Management,* 11:2, 1-12, DOI: dx.doi.org/10.4314/iijikm.v11i2.1

Osayande, O. (2009).“Security issues in academic libraries: the way out.”*Jolis*, 6(1), 103-118. https://www.academia.edu/26805973/security issues in academic libraries the way out

Osayande, O. (2011). “Electronic Security systems in Academic libraries: A case study of three university libraries in South West Nigeria.” *Chinese librarianship, an international electronic journal*, 32. Retrieved from: http://www.ick.us/cliej/cl32osayande.pdf

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

Oyesiku, F.A, Buraimo, O & Olusanya, O.F. (2012). Disruptive readers in academic libraries: A Study of Olabisi Onabanjo University Library. Retrieved from http://unllib.unl.edu/LPP/

Oyewusi, F.O., & Oyeboade, S.A. (2009). An empirical study of accessibility and use of librarr resources by undergraduates in a Nigerian state university of technology. *Library Philosophy and Practice.* http://unllib.unl.edu/LPP/oyewusi-oyeboade.htm

Ozowa. V., Aba, J & Aba.T (2016). Impact of Electronic Surveillance Systems on

Theft and Mutilation in Francis Suleimanu Idachaba Library, University of Agriculture Makurd.Library Philosophy and Practice , 1-17. http://digitalcommons.unl.edu/libphilprac/1429

Person, R. L. (2007). Electronic Security Systems: A Manager's Guide to Evaluating and Selecting System Solutions. Amsterdam: Butterworth-Heinemann

Powell, A. & Gillet, M. (2007). "Controlling Access in the Electronic Library." *Ariadne*, 7. Available at http://www.ariadne.ac.uk/issue7/access- control

Purtell, T (2007). "A new view on IT risk." *Risk Management,* 54 (10-11), 26-31. https://doi.org/10.1016/j.ejor.2015.12.023

Rajendran, L. & Rathinasabapathy, G. (2007). Role of Electronic Surveillance and Security Systems in Academic Libraries. Retrieved from http://www.library.lgcar.gov. in/readit/2007/compros/s4 2pdf.

Rathinasabapathy, G. & L. Rajendran(2015), "RFID Technology and Library Security: Emerging Challenges*." Journal of Library, Information, and Communication Technology*,1 (1), 34-43. https://www.researchgate.net/publication/265353875

Ridley, J. & Pearce, D. (2006). Safety with machinery, Boston: Elsevier.

Roper, J.A., Grau, J.A. & Fischer, L.F. (2005) Security education, awareness and training: From theory to practice, New York: Elsevier

Saffady, W. (2005). ''Risk analysis and control: Vital to records protection.'' *Information Management Journal*, 39 (5): 62-64.

Salaam, M .O. & Onifade. ((2010). "The perceptions and attitude of students in relation to vandalism in Nimbe Adedipe library, university of agriculture Abeokuta." *Library and Archival Security*.24(2).http://nopr.niscair.res.in/bitstream /123456789/9751/4/ALIS%2057%282%29%20146-149.pdf

Sargent. C (2001). ''Two sixteenth-century book lists from the library of queens' college, Cambridge.'' *Transactions of the Cambridge Bibliographical Society*, 12(2) 161-178: https://www.jstor.org/stable/41154906

Schmidts, A. & Lian, S. (2009). Security and Privacy in Mobile Information and Communication Systems. Turin, Italy: Springer.

Schuessler, J.H. (2009). "General deterrence theory: Assessing information systems security effectiveness in large versus small businesses." *University of NorthTexas.* ttp://joseph.schuesslersounds.com/Research/Dissertation/Schuessler_Dissertati on.pdf, (accessed May 10, 2019).

Shafack, R. (2021). "Securing Library and Information Resources: The Situation in Two State University Libraries in Cameroon." *European Journal of Education and Pedagogy, 2*(1), 25-31. https://doi.org/10.24018/ejedu.2021.2.1.13

Shaluf, I. (2007). "Disaster types." *Disaster prevention and management,*

16 (5), 704-717. http://dx.doi.org/10.1108/09653560710837000

Shameenda.K.L (2011). Preservation and Conservation of Library Materials, Techniques and Practices: A Case Study of the University of Zambia Libraries. Unpublished. Available at : http://dspace.unza.zm › bitstream › handle

Shamsul. K. W. F, et al (2012).“ Information Security Awareness Amongst Academic Librarians.”*Journal of Applied Sciences Research*, 8(3): 1723-1735. file:///C:/Users/Hp/Downloads/1723-1735.pdf

Silic, M & Back, A. (2014). “Information security: critical review and future directions for research.” *Inf.Manag. Comput. Secur*., 22 (3), 279–308. doi:10.1108/ IMCS-05-2013-0041.

Simui, M. (2004). The provision of Scholarly Information in Higher Education in Zambia. African Universities in the twenty-first century. Volume II. Knowledge and Society.

Simui, M. & Kanyengo, C.W. (2001). An Investigation into the funding of University Libraries in Zambia´ unpublished report.

Simukali.M.C (2019). multi factor authentication access control for student and staff based on rfid, barcode and gis. Available at: http://dspace.unza.zm/handle/123456789/6623

Singh, D. (2007). ‘’The role of the academic library in facilitating research: perceptions of postgraduate students.’’ *Library management*, 5 (2) 26-27. file:///C:/Users/Hp/Downloads/The role of academic libraries in facilitating_pos%20(3).p df

Soria, K.M., Fransen, J., & Nackerud, S. (2016). “Beyond books: the extended academic benefits of library use for first-year college students.” *College & Research Libraries*, 78 (1), 8-22, (available at: doi:10.5860/crl.78.1.8 (Accessed March 7, 2019).

Soria, K.M., Fransen, J. & Nackerud. S. (2017). “The impact of academic library resources on undergraduates’ degree completion.*” College & Research Libraries*, 78 (6), 812-823. Available at: doi: 10.5860/crl.78.6.812, (accessed March 7, 2019).

Soomro, Z.A., Shah, M.H. & Ahmed, J. (2016). “Information security management needs more holistic approach: a literature review.” *Int. J. Inf. Manag*. 36 (2), 215–225. doi:10.1016/j.ijinfomgt.2015.11.009.

Sundt, C. (2006). “Information security and the law, Information Security Technical Report.” 11 (1), 2-9: http://www.sciencedirect.com/science/journal/13634127

Spagnoletti, P & Resca, A. (2008). ‘’The duality of information security management: Fighting against predictable and unpredictable threats.’’ *Journal of Information Security*, 4(3), 46 - 62.

Tiwari,B. K & Sahoo, K.C (2013). "Infrastructure and Use of ICT in University Libraries of Rajasthan (India)" (2013). *Library Philosophy and Practice (e-journal*). 883. https://digitalcommons.unl.edu/libphilprac/883

Trapskin, B. A. (2008). “Changing of the guard: Emerging trends in public library security.” *Library and Archival Security*,21 (2), 69-76. https://doi.org/10.1080/01960070802201359

Treptow, R. & James, M. (2011). “Use of online knowledge resources by prominent South African researchers.” *South African Journal of Libraries and Information Science*, 77 (1), 64-74. DOI: https://doi.org/10.7553/77-1-67

Turle, M. (2008).“Data security: Past, present and future.” *Computers & Security*, 25, 51-58.

Udoumoh, C. N., & Okoro, C. C. (2007). “The Effect of Library Policies on Overdue Materials in University Libraries in Southern Nigeria.” *Library Philosophy and Practice*, *9*(2), 35-142. https://digitalcommons.unl.edu/libphilprac/142

UNESCO, (2015). ‘’Empowering Information Professionals: A training programme on information and communication technology.’’ *Introduction to Library Automation Student’s Text*. Retrieved from http://www.unescobkk.org/elib/ publications/ICTEIP/MODULE2/ICTEIP_MOD2_ppt/ICTEIP_MOD2_L1.pdfa

Unisys. (2007). Unisys Security Index Malaysia: A Synovate Survey, available at: ttp://www.unisys.com.sg/eprise/main/admin/country/doc/sg/MY_Security_Ind (Accessed April 2, 2019).

University of Zambia Annual Report, (2005). Lusaka, University of Zambia

Urhiewhu1. O. L, Emojorho. D & Omah.E.J (2018). “security measures adopted to prevent theft of library resources in selected academic libraries.”*International Journal of Library and Information Science Studies*, 4 (1) :www.eajournals.org. (Accessed October, 2018).

Vacca, J.R. (2009). Computer and information security handbook, Burlington: Morgan Kaufmann Publication.

Vellani, K. H. (2010). Crime Analysis for Problem Solving Security Professionals in 25 Small Steps. Retrieved from www.popcenter.org/library/reading/pdfs/crimeanalysis25steps.pdf

Wambiri, D. (2008). Disaster planning and Preparedness in University Libraries in Kenya. PhD Thesis. School of Information Science. Moi University, Eldoret, Kenya. http://ir.mu.ac.ke:8080/xmlui/bitstream/handle/123456789/362/ Tanui%20Vincent%20Kipruto%202013.pdf?sequence=1&isAllowed=y

Wamunyima K, C. (2009), "Meeting collection development needs in resource poor settings: the University of Zambia Medical Library experience", *Collection Building*, 28 (1). 26-30. https://doi.org/10.1108/01604950910928484

Webb, P. J. (2007). Providing effective library services for research. London: Facet Publishing.

Weiner, S. G (2005), " The History of Academic Libraries in the United States: a Review of the Literature". *Library Philosophy and Practice* (e-journal). 58. https://digitalcommons.unl.edu/libphilprac/58

Yeh, Q.-J. & Chang, A.J.-T. (2007). “Threats and countermeasures for information system

security: a cross-industry study." *Inf. Manag*., 44 (5), 480–491. doi:10.1016/j.im. 2007.05.003

Young, J. C. et al (2021). "Public Libraries and Development across Sub-Saharan Africa: Overcoming a Problem of Perception" *Libri*,71 (4). 419-429. https://doi.org/10.1515/libri-2020-0096

Zimerman, M. (2010). "Protect your library's computers." *New Library World*, 111(5/6), 203-212. doi:10.1108/03074801011044070

INTERVIEW GUIDES INTERVIEW GUIDE FOR CIRCULATION LIBRARIAN THE UNIVERSITY OF ZAMBIA

DIRECTORATE OF RESEARCH AND GRADUATE STUDIES

Dear respondent,

I am a post-graduate student at the University of Zambia (UNZA) pursuing a Master's Degree in Library and Information Science. I am currently conducting a study on "***Security measures adopted to prevent theft of library resources in selected academic libraries in Zambia***". You have been purposively selected to participate in this research. Be assured that the responses you give will be treated with the utmost confidentiality and only for this research.

Thank you for accepting to be a respondent.

Researcher

Date_____

The interview guide will be used to collect information from Circulation Librarians on issues about disaster preparedness and mitigation for computer-based information systems in libraries.

My name is Bestain Hampwaye

The purpose of the interview is to find out about the security systems being used in your library

1. Gender:_____
2. Age:_____
3. Academic Qualification:_____
4. Position_____
5. Name of library_____

Interview questions

6. How long have you worked in this library?.....
7. Have you ever had any theft or mutilation of print materials in your library?.....
   a.If so, what type of print materials are most vulnerable?.....
   b. what measures have put in place to control this problem?
   c. are the measures put in place effective?
8. Does the library have a cloak room or safe place where library users keep their Belongings?.....
   a. If so, what security measures have you put in place to protect people's items? .....
   b. Are the measures effective?.....
   b. If not, do you allow library users to go inside the library with their belongings like bags?……
9. Have you ever received any complaints from library users where they have lost their items in the library? .....
   a. If so, which items do they lose most?.....
   b. How frequently do you receive such reports?
   b. If not, how have managed to control this? .....
10. Do you put security features to your print materials to establish ownership?
    a. If yes, what are those security features?
    b. where do you put these features?.....
    c. How effective are they?.....
11. Do you have written policies, rules, and procedures related to collection access, use, controls and protection formulated by the various departments involved in the life cycle of library collections?

a. If yes, what are some of the rules and procedures regarding collection access, use, controls, and protection?

b. Are these rules and procedures documented and understood by all staff and users?

c. How effective are they?

12 Do the library take regular collection inventory and report to ascertain total collection, detect security threats (lost, misplaced, theft, decayed, damaged items).

a. If yes. How regularly do undertake that?

b. If no, how do you know the lost materials?

13. Are there organised activities and training being offered to increase staff and user awareness of security issues?

a. how regular are these trainings conducted

b. who conducts these trainings?

C. are they effective

14. What do the students and staff required to produce when entering the library?

15. What rules and procedures have you put in place to access restricted areas like short loan during and after opening hours?

16. Are all OPAC stations protected from unauthorised access (through passwords and user IDs)?

17. Have you ever experienced where borrowed books or items are not returned by borrowers?

a. If yes, what causes some of the items not to be returned?

b. What measures have you put in place to ensure that such items are returned?

c. If no, what measures have you put in place to control this?

18 Have you ever experienced a situation where books are wrongly shelved deliberately by library users?

a. If yes, what do you think library users do that?

a. If no, what security measures have you put in place to control this problem?

19. Have you ever caught a library user borrowing books using someone else's ID without permission?

a. If yes, what could be the reason for the user to behaviour that way?

a. How do you deal with such people?

b. If not, what control measures have been put in place?

20. Do you at times face challenges where staff allow friends, family members to borrow restricted item with or without proper borrowing?.....

21. What security measures have you put in place to protect library materials when there is power outages especially in the night?.....

    b. What effects does this have on the library operations and services?.....

    c. Was there a time when the library was unable to control the situation?.....

    d. How did this affect the library?.....

    e. If no, why do you think this has been the case?.....

22. In your opinion what are the major challenges affecting the security management of the library materials?.....

23. What are security measures has the library put in place to ensure the security of its library materials such as books?.....

24. Any other information or comment you may wish to add is most welcome……

End of interview

INTERVIEW GUIDE FOR INFORMATION SYSTEMS LIBRARIAN AND IT MANAGER

THE UNIVERSITY OF ZAMBIA

DIRECTORATE OF RESEARCH AND GRADUATE STUDIES

Dear respondent,

I am a post-graduate student at the University of Zambia (UNZA) pursuing a Master's Degree in Library and Information Science. I am currently conducting a study on "***Security measures adopted to prevent theft of library resources in selected academic libraries in Zambia***". You have been purposively selected to participate in this research. Be assured that the responses you give will be treated with the utmost confidentiality and only for this research.

Thank you for accepting to be a respondent.

Researcher

Date_____

The interview guide will be used to collect information from the Information Systems Librarians and ICT managers on issues about security problems and mitigation for computer-based information systems in libraries.

My name is Bestain Hampwaye

The purpose of the interview is to find out about the security systems being used in your library

1. Gender: a) Male [ ] b) Female [ ]

2. Age: a) Below 30years [ ] b) 31-40 years [ ] c) 41-50 years d) above 50 years [ ]

3. a) Qualifications: PhD [ ] b) Master's Degree [ ] c) Bachelor's Degree [ ] d) Diploma and Certificate [ ]

Interview questions

4.Name of Organization……

5. Position…….

6. How long have you worked in this institution?.....

7 Does the library offer online services?.....

8. In your opinion what does security for information system entail?.....

9. What measures have you put in place to ensure the security of the computer-based information systems?.....

10. If any, how effective is the security system?.....

11. In your own opinion, do you think your library is well prepared to handle security problems or any problem that might affect the library?.....

a. If so, how?.....

b. If no, why not?.....

12. Kindly explain the support given by the top management to ensure the security of information system?.....

13. Are there written policies and programmes that focus on security management for information system in the library?.....

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 before approval?.....

i. If no, why not?.....

14. What role do you play in ensuring the security of computer-based information system (CBIS)

and Role in Database Management of (CBIS)?.....

15. Are they well defined in your contract?.....

16. Do you have any training focusing on security in database management?.....

a. If so, which one?.....

b. If not, do you think it is necessary to be trained on security management for CBIS?.....

c. If so, what have you done towards this goal?.....

17. 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 the likelihood that the library will experience any security problem that may affect its CBIS? Please explain your answer?……

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

19. 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?.....

20. Who maintains library CBIS?.....

21. Any other information or question you may wish to add is most welcome?……

End of interview

INTERVIEW GUIDE FOR ACADEMIC LIBRARIAN / DEPUTY LIBRARIAN
THE UNIVERSITY OF ZAMBIA

DIRECTORATE OF RESEARCH AND GRADUATE STUDIES

Dear respondent,

I am a post-graduate student at the University of Zambia (UNZA) pursuing a Master's Degree in Library and Information Science. I am currently conducting a study on "***Security measures adopted to prevent theft of library resources in selected academic libraries in Zambia***". You have been purposively selected to participate in this research. Be assured that the responses you give will be treated with the utmost confidentiality and only for this research.

Thank you for accepting to be a respondent.

Researcher

Date_____

The interview guide will be used to collect information from the academic
Librarians on issues pertaining to security problem and mitigation against the problems in libraries.

The purpose of the interview is to find out about the security systems being used in your library.

1. Gender: a) Male [ ] b) Female [ ]

2. Age: a) Below 30years [ ] b) 31-40 years [ ] c) 41-50 years d) above 50 years [ ]

3. a) Qualifications: PhD [ ] b) Master's Degree [ ] c) Bachelor's Degree [ ] d) Diploma and Certificate [ ]

Interview questions

4. Name of library.....……

5. Position…….....

6. How long have you worked in this institution?.....

7. Does the library have security system in place?.....

8. If it does, what type of security system does it have in place?……

If not, how does the library ensure that its resources are secure?.....

9. In your opinion what is the importance of security system?.....

10. Has the library experienced any security problem before?.....

a) Yes [ ] b) 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 security measures has the library put in place to mitigate or reduce the occurrence of such problems?.....

11. If the library has not experienced any security problem affecting its operations, what has contributed to this success?.....

12. Does your library have a security management team?.....

a. If yes who are the members of this security management team?.....

b. what are the functions of the security management team?.....

13 How does the library ensure security of its library staff, users and other library materials?.....

14. In your opinion, what role does the University or College management play in security management in the library (Budget, policies, programmes, strategic plan, and training?...

15. What personnel are in-charge of security management in the organization?.....

16 Do they have defined roles and responsibilities?.....

17. Does the library have any programmes, policies that focus on security management?

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?.....

18. What are the challenges or hindrances encountered in ensuring security in the Library?.....

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

20. Any other thing you may wish to add in regard to this study is welcome?……

End of interview