SCHOOL OF LIBRARY ARCHIVES AND DOCUMENTATION STUDIES

SLADS_BAGAMOYO

RESEARCH PROPOSOL

ASSESSMENT OF CYBER SECURITY THREATS ON MANAGEMENT OF ARCHIVES IN TANZANIA, A CASE STUDY IN ARCHIVES

BY

DEVIS MALIUS SINKALA

NS2927/0053/2022

A Research Report Submitted at the School of Library, Archives and Documentation Studies for the Partial Fulfillment of the Requirement Award of Ordinary Diploma in Records and Archives Studies

2026

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

CERTIFICATION

The undersigned certifies that he/she has read and hereby recommends for acceptance by the School of Library, Archives and Documentation Studies (SLADS), a research report entitled"**Assessment of cyber Security Threats Affecting the Management of Archives in Tanzania."**This report is submitted in partial fulfillment of the requirements for the award of the Ordinary Diploma in Records and Archives Management.

Supervisor's Name

SIR CHRISTOPHER GWALUGWA

Signature:

.....

Date

.....

-

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

DECLARATION AND COPYRIGHT

DEVIS MALIUS SINKALA i declare that this research report is my own original work and has not been submitted to any other institution for academic award or examination purposes. All sources of information used in this study have been duly acknowledged through appropriate citations and references.

Signature:

.....

Date:

.....

Copyright © (2026) **DEVIS M. SINKALA**

This research report is copyright material protected under the Berne Convention, the Copyright Act, 1999 and other international and national laws relating to intellectual property rights. No part of this report may be reproduced, stored, or transmitted in any form or by any means without prior written permission of the School of Library, Archives and Documentation Studies (SLADS), except for brief quotations used for research, private study, or scholarly review with proper acknowledgement.

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

DEDICATION

This research report is dedicated to my beloved parents, family members, friends, and everyone who provided encouragement, prayers, guidance, and moral support throughout my academic journey. Their continuous support greatly contributed to the successful completion of this study.

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to Almighty God for granting me good health, wisdom, strength, and guidance throughout the preparation of this research report.My heartfelt appreciation goes to my supervisor, Sir Christopher Gwalugwa, for his valuable guidance, constructive comments, encouragement, and continuous support throughout the preparation of this research report.

I also sincerely thank all respondents and institutions that participated in this study for their cooperation during data collection. Finally, I extend my sincere appreciation to my family and friends for their prayers, encouragement, and moral support throughout this study.

May Almighty God bless you all abundantly.

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

LIST OF ABBREVIATIONS AND ACRONYMS

ICT	Information and Communication Technology
ITU	International Telecommunication Union
NIST	National Institute of Standards and Technology
TNA	Tanzania National Archives
UNESCO	United Nations Educational, Scientific and Cultural Organization
SLADS	School of Library, Archives and Documentation Studies
RAM	Records and Archives Management
ICT	Information and Communication Technology

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

ABSTRACT

This study assessed the cyber security threats affecting the management of archives in Tanzania. The study was guided by four specific objectives: to identify the main types of cyber security threats affecting archival information systems in Tanzania, to evaluate the current practices and institutional measures used to safeguard archives against cyber threats, to assess staff awareness and preparedness for cyber security risk management within archival institutions, and to propose strategies for improving cyber security in archives management.The study employed a mixed methods research approach and a descriptive research design. Data were collected through questionnaires and interviews from a sample of 18 respondents drawn from archival institutions in Tanzania. Quantitative data were analyzed using descriptive statistics, particularly frequencies and percentages, while qualitative data were analyzed through thematic analysis.The findings revealed that archival institutions face several cyber security threats, including malware attacks, phishing, unauthorized access, weak passwords, and inadequate cyber security awareness among staff. The study further found that although some institutions had implemented cyber security measures such as antivirus software, firewalls, and password protection, challenges including inadequate staff training, outdated systems, and limited cyber security policies continued to expose archival information to cyber risks.The study concludes that strengthening cyber security policies, improving staff awareness through regular training, investing in modern security technologies, and conducting continuous monitoring of information systems are essential for enhancing the security and effective management of archives in Tanzania. The findings are expected to contribute to strengthening cyber security practices and protecting archival information within Tanzanian archival institutions.

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

TABLE OF CONTENTS

CERTIFICATION..... i

DECLARATION AND
COPYRIGHT ii

DEDICATION iii

ACKNOWLEDGEMENT iv

LIST OF ABBREVIATIONS AND
ACRONYMS v

ABSTRACT vi

TABLE OF
CONTENTS vii

LIST OF
TABLES viii

LIST OF
FIGURES ix

CHAPTER ONE 14

INTRODUCTION AND BACKGROUND OF THE STUDY 16

1.0 Introduction 16

1.1Background and Rationale 16

1.2 Statement of the Problem 18

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

1.3 Objectives of the study 19

1.3.1General Objective 19

1.3.2 Specific Objectives 19

1.4 Research Questions 19

1.5 Significance of the Study 20

1.6 Scope of the Study 20

1.7 Limitations of the Study 21

CHAPTER TWO 23

LITERATURE REVIEW 23

2.0 Introduction 23

2.1. Meaning of concepts 23

2.1.1Specific indicators security threats on management of archives in Tanzania 24

2.2 Theoretical framework 25

2.3. Common Cybersecurity Threats Identified in Empirical Studies 25

2.3.1 Effects of Cybersecurity Threats on Archive Management 26

2.4 Research gap 26

2.6 Conceptual Framework 27

CHAPTER THREE 28

RESEARCH METHODOLOGY 28

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

3.0 Introduction 28

3.1 Research Design 28

3.2 Area of the study 29

3.3 Population of the study 29

3.4 Targeted population 29

3.5 Sample Size: 30

3.6 sampling technique 30

3.6.1 Purposive sampling 30

3.6.2 Simple random sampling 30

3.7 Data Collection Methods 31

3.7.1 Quantitative data analysis 31

3.8 Ethical Consideration 32

CHAPTER FOUR 33

DATA ANALYSIS, PRESENTATION AND DISCUSSION 33

4.1 Introduction 33

4.1.1 Questionnaire Response Rate 33

4.2 Respondent's Demographic Details 34

4.2.1 Respondents Age 34

Figure 1: Age of Respondents (N = 18) 35

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

4.2.2 Respondents Gender 35

Figuree 2: Gender of Respondents (N = 18) 36

4.2.3 Education Level of Respondents 37

Figure 3: Education Level of Respondents (N = 18) 37

4.2.4 Years of Experience 38

Figure 4: Years of Experience of Respondents (N = 18) 38

4.3 Types of Cyber Security Threats Affecting Archives 39

Table 1: Main Type of Cyber Security Threat Experienced (N = 18) 39

4.3.1 Frequency of Cyber Security Threats on Archives 41

Table 2: Frequency of Cyber Security Threats (n = 18) 41

4.3.2 Most Weak Areas of Archival Information to Cyber Threats 42

Table 3: Most Weak Areas of Archival Information (N = 18) 42

4.4 Existing Cyber Security Measures Used in Archives 44

Table 4: Existing Cyber Security Measures in Archives (N = 18) 44

4.4.1 Effectiveness of the Existing Cyber Security Measures 45

Table 5: Effectiveness of Existing Cyber Security Measures (N = 18) 46

4.4.2 Review and Update of Cyber Security Policies 47

Table 6: Frequency of Review and Update of Cyber Security Policies (n = 18) 47

4.5 Staff Awareness and Preparedness on Cyber Security 48

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

Table 7: Staff Training on Cyber Security Risks (N = 18) 48

4.5.1 Staff Confidence in Handling Cyber Security Incidents 49

Table 8: Staff Confidence in Handling Cyber Security Incidents (N = 18) 49

4.5.2 Clarity of Roles and Responsibilities in Managing Cyber Security Risks 50

Table 9: Clarity of Roles and Responsibilities in Cyber Security Management (N = 18) 51

4.6 Strategies for Improving Cyber Security in Archive Management 52

4.6.1 Regular Staff Training and Awareness Programs 52

4.6.2 Implementation of Strong Access Control and Authentication 53

4.6.3 Regular Updating of Antivirus Software and Systems 53

4.6.4 Development of Institutional Cyber Security Policies 54

4.6.5 Regular Backup of Archival Data 54

4.7 Chapter Summary 55

CHAPTER FIVE 56

SUMMARY, CONCLUSION, AND RECOMMENDATIONS 56

5.0 Introduction 56

5.1 Summary of the Findings 57

5.2 Conclusion 58

5.3 Recommendations 59

5.4 Recommendations for Further Studies 59

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

REFERENCES 60

APPENDIX I 64

RESEARCH QUESTIONNAIRE 64

APPENDIX II 67

INTERVIEW GUIDE 67

APPENDIX I 68

REAEARCH WORK PLAN/ SCHEDULE TIME FRAME 68

APPENDIX II 69

BUDGET 69

APPENDIX III 70

APPROVAL LETTER 70

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

LIST OF TABLES

Table 4.1: Main Type of Cyber Security Threat Experienced 23

Table 4.2: Frequency of Cyber Security Threats 25

Table 4.3: Most Weak Areas of Archival Information 26

Table 4.4: Existing Cyber Security Measures in Archives 28

Table 4.5: Effectiveness of Existing Cyber Security Measures 29

Table 4.6: Frequency of Review and Update of Cyber Security Policies 30

Table 4.7: Staff Training on Cyber Security Risks 31

Table 4.8: Staff Confidence in Handling Cyber Security Incidents 32

Table 4.9: Clarity of Roles and Responsibilities in Cyber Security Management 34

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

LIST OF FIGURES

Figure 4.1: Age of Respondents 19

Figure 4.2: Gender of Respondents 20

Figure 4.3: Education Level of Respondents 21

Figure 4.4: Years of Experience of Respondents 22

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

CHAPTER ONE

INTRODUCTION AND BACKGROUND OF THE STUDY

1.0 Introduction

This chapter comprises of the following aspects; background to the study, statement of the problem, objectives of the study, research questions, significance of the study, scope of the study and limitations of the study as well as definitions of key terms.

1.1Background and Rationale

In the digital era, archival records increasingly exist in electronic formats and are managed using information systems connected to networks and the internet. While digital archives improve access and preservation, they also expose archival systems to a range of cyber security threats such as hacking, malware, ransom ware, and data breaches. Archives risk loss of integrity, confidentiality, and availability of records (kagendo,2020). if cybersecurity threats are not adequately addressed. Studies in other African contexts show digital repositories face frequent phishing, password attacks, malware, and denial of service attacks that can compromise archival data and services. (Albrecht and McGleen,2020)

In Tanzania, cybersecurity research has focused on e-government systems and public sector vulnerabilities, revealing significant challenges in cyber literacy, infrastructure, and policy frameworks(Mwalimu,2022). These broader cybersecurity gaps underscore the urgency of investigating how archival institutions are similarly threatened and how they manage these threats to protect archival assets so it make big function to handle those archives within their archival institution instead of they are most important in order for enhancing work flow efficiency so In recent decades, public and private institutions around the world have increasingly adopted digital technologies to store,

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

manage, and provide access to information and records(Smith and Johnson,2021). Archives — once primarily paper-based repositories now hold large volumes of digitally created and digitally stored records, making them part of a broader digital information ecosystem vulnerable to modern cyber risks. As ICT reliance grows, so does the spectrum of security threats, including phishing, malware, ransomware, and unauthorized access attempts that target digital systems and networks. These attacks can compromise confidentiality, integrity, and availability of digital records, disrupt archival services, and undermine trust in records systems worldwide. Within the archival profession, digital security concerns are already recognized internationally. For example, research on the cyber-security of the National Archives and Records Service of South Africa shows that archival information systems face a wide variety of cyber-attacks such as phishing attempts, Trojan horses, computer viruses, and denial of service attacks, which can damage systems and threaten vital information holdings. Mitigation measures such as firewalls, passwords, and antivirus software are used, but gaps in practices and policies often remain.

In Tanzania, digital transformation is a key component of national development priorities, supported by legislation and ICT strategy frameworks intended to enable e-government, digital recordkeeping, and secure online services. The government has enacted various laws and is building institutional capacity to respond to cyber threats, and has invested in digital forensics training and cybersecurity policy frameworks to strengthen national resilience (Tanzania Data Protection Act 2021).

Despite progress, cybersecurity weaknesses persist in many Tanzanian public institutions. National audit reports have identified gaps in basic cybersecurity practices—including inadequate vulnerability assessments, weak access controls, poor incident management, and inconsistent implementation of cyber strategies which leave systems vulnerable to attacks (Nyerere and Chacha,2022).

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

Although these issues are documented for government systems generally, there is limited empirical research focusing on the particular context of archives and records management in Tanzania — even as archives increasingly rely on digital platforms and systems for long-term preservation, access and service delivery.

Tanzania Cybercrimes Act of 2015 criminalizes unauthorized access to computer systems and data, showing a domestic legal foundation for addressing cyber threats, yet the applicability of such frameworks to archives and records institutions remains under-explored.

1.2 Statement of the Problem

Archives in Tanzania should be completely secure from cyber security threats. They are essential for preserving important historical records, legal documents, and other crucial information. Proper management of these archives ensures that they remain safe, accessible, and protected from unauthorized access and cyber-attacks (Sithole & Mjema, 2021

Many archives in Tanzania lack the necessary resources, trained personnel, and modern technology to defend against cyber threats effectively (Mhando, 2022). Studies indicate that cyber-attacks on cultural and historical institutions are increasing globally, and Tanzania is no exception. The archiving sector often faces challenges such as limited budget allocations, insufficient infrastructure, and a lack of awareness about cyber risks (Mwanza, 2023). As a result, many archives remain vulnerable to breaches that could lead to the loss or manipulation of vital information.

Vulnerabilities can be dire because when archives are compromised, there is a risk of losing important historical evidence, which can impact national identity and heritage (Ngatunga, 2023). Additionally, unauthorized access to sensitive documents can result in legal disputes, loss of public trust, and difficulties in governance (Chimwaga, 2022). Given these significant risks, understanding and addressing the cyber security threats

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

facing archives in Tanzania is crucial for both preserving the nation's history and ensuring the integrity of government operations.This research aims to assess the specific cyber security threats to archive management in Tanzania, comparing the current challenges to the ideal standards of protection, and to highlight the urgent need for improved measures in this critical area.

1.3 Objectives of the study

1.3.1General Objective

To assess cyber security threats affecting the management of archives in Tanzania and develop recommendations to enhance archival security.

1.3.2 Specific Objectives

1. To identify the main types of cyber security threats affecting archival information systems in Tanzania

2. To evaluate current practices and institutional measures for safeguarding archives against cyber threats.:

3. To assess staff awareness and preparedness for cyber security risk management within archival institutions

4. To propose a strategic framework for improving cyber security in archives management.

1.4 Research Questions

1. What are the prevalent cyber security threats facing archival systems in Tanzania?

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

2. What best practices can be recommended to strengthen archival cyber security?

3.How effective are current cyber security measures in protecting these archives?

1.5 Significance of the Study

This research will be provided valuable insights for archival institutions, policymakers, and ICT managers in the cultural heritage sector in Tanzania. It was informed policy development, staff training programmers, and implementation of security measures that protect archival assets from cyber threats. The study of cybersecurity threats impacting the management of archives in Tanzania is significant for several reasons, Protection of Vital Historical and Administrative Records: Archives contain crucial historical, legal, and administrative information. Understanding cybersecurity threats helps safeguard these records against hacking, data breaches, and loss, ensuring national heritage preservation (Brown & Smith, 2022),Enhancement of Data Security Protocols: Research identifies vulnerabilities within archival management systems, leading to improved security measures that prevent unauthorized access and cyberattacks (Kagwa & Mwakalinga, 2023), Supporting Government Transparency and Accountability: Secure management of archives promotes transparency by ensuring government documents are protected from cyber threats, thus fostering trust and accountability (Mkapa, 2022), Aligning with Digital Transformation Goals:

1.6 Scope of the Study

The scope defines the boundaries within which the research was be conducted:

The study concentrates on archives management institutions in Tanzania, including government archives, private record-keeping organizations, and academic institutions' archives (Wainaina et al., 2021). It specifically assesses cyber security threats affecting the integrity, confidentiality, and availability of digital archives. This includes threats

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

such as malware, phishing, unauthorized access, and data breaches (Kumari & Kesar, 2020), Time Frame: The research focuses on current cyber security threats and trends observed within the last five years to ensure relevance (Njuguna et al., 2022),Methodology, the study employs qualitative and quantitative methods, including surveys, interviews, and case studies involving key personnel responsible for archives management.

1.7 Limitations of the Study

Access to Data:

Some archives may be reluctant to share sensitive information regarding their cyber security measures or incidents due to confidentiality concerns, limiting data comprehensiveness (Mtega & Mtega, 2020).

Resource Constraints

Financial and technological limitations may restrict the ability to perform extensive technical assessments of the cyber security infrastructure within Tanzanian archives. Rapidly Evolving Threat Landscape, Cyber threats are continuously evolving, which could render some findings outdated shortly after the study completion (Almarash et al., 2023)

Sample Size and Generalizability

Due to logistical constraints, the sample size may be limited, impacting the generalizability of findings across all archives in Tanzania.

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

Literature review is a written summary of journal articles, books and other documents like conference papers and government documents that describes the past and current state of information on the topic of your research study (Creswell, 2013). It covers definition of key terms, Theoretical literature review, empirical literature review, Research gap and conceptual framework. This review explores previous research related to the cybersecurity threats faced by archives in Tanzania, highlighting key findings, researchers, and existing gaps in the literature.

2.1. Meaning of concepts

a) Assessment

Assessment is the systematic process of examining and evaluating a situation, problem, or system to determine its effectiveness, strengths, weaknesses, and areas that need improvement (Creswell & Creswell, 2018).

b) Cyber Security

Cyber security is the protection of computer systems, networks, digital information, and electronic records from unauthorized access, cyber-attacks, damage, theft, or disruption

c) Cyber Security Threats

Cyber security threats are potential dangers or malicious activities such as hacking, malware, phishing, ransomware, data breaches, and unauthorized access that can compromise the confidentiality, integrity, and availability of digital information (NIST, 2024).

d) Archives Management

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

Archives management is the process of identifying, preserving, organizing, protecting, and providing access to archival records with enduring value to ensure they remain authentic, reliable, and accessible over time (International Council on Archives, 2016).

2.1.1Specific indicators security threats on management of archives in Tanzania

(a) Ransomware Incidents, Reports of ransomware attacks impacting archives, where data is encrypted and held for ransom, disrupting access and preservation efforts.

(b)Unauthorized Access Attempts, Evidence of unauthorized access to digital archives, whether through brute force attacks on passwords or exploitation of unsecured systems.

(c) Data Loss or Corruption, Instances of data corruption or loss linked to cyber incidents, including malware infections that compromise archived materials.

(d) Insider Threats, Cases of insider threats, were employees or contractors misuse access to sensitive archival data for malicious purposes or negligence, leading to data exposure.

(e)Vulnerable Software and Systems, use of outdated software and unsupported systems in archive management, which may have known vulnerabilities exploited by cybercriminals.

(f)Inadequate Cybersecurity Protocols, Lack of comprehensive cybersecurity policies, training, and awareness among staff responsible for managing archives, increasing the risk of human error.

(h)Increased Use of Cloud Services, Migration of archives to cloud services without proper security assessments, posing risks related to data breach and loss of control over sensitive information.

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

2.2 Theoretical framework

Systems Theory

Systems theory examines the interrelated components within a whole and how they interact with each other and their environment so due this can help in understanding the archival ecosystem in Tanzania, including technology, processes, human factors, and external threats. It can guide the identification of vulnerabilities and assess the overall resilience of archive management systems.

Diffusion of Innovations Theory

This theory, developed by Everett Rogers, explains how new ideas and technologies spread within and between societies so this framework can be used to investigate how advancements in cyber security technologies are adopted by archival institutions in Tanzania. It can also explore barriers to adopting best practices in cyber security.

Risk Management Framework

This framework involves identifying, assessing, and prioritizing risks followed by coordinated efforts to minimize, monitor, and control the probability of unfortunate events this is vital for assessing the specific cyber security threats that archives in Tanzania face and determining how effective their current risk mitigation strategies are.

2.3. Common Cybersecurity Threats Identified in Empirical Studies

System Vulnerabilities due to Studies on Tanzanian e-government systems found, cross-site scripting vulnerabilities in ~50% of systems so denial-of-service a but Implication for archives ,Digital archival systems can be accessed, altered, or destroyed

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

through similar vulnerabilities, Low Cybersecurity Awareness this means research shows low cyber literacy among government staff significantly increases exposure to attacks so For archives: Poor handling of passwords, phishing emails, or storage systems can lead to ,Unauthorized access and Loss of confidential records, Network and Infrastructure Weaknesses means that Case studies (e.g., institutional Wi-Fi security in Tanzania) highlight weak configurations and insecure access points and Impact on archives are like Weak networks expose archival databases to Hacking, Data interception and Unauthorized duplication, Malware,

2.3.1 Effects of Cybersecurity Threats on Archive Management

Empirical evidence suggests several impacts which are like Loss of Data Integrity due to Unauthorized modification of records undermines authenticity and reliability of archives, Reduced Accessibility means that Cyber-attacks (e.g., DoS) can make archives unavailable for users and researchers, Confidentiality Breaches includes sensitive government or institutional records may be exposed, Operational Disruption means that cyber incidents slow down records management processes and service deliver, Financial and Reputational Damage due to Tanzania has previously suffered large financial losses due to cybercrime Act 2015

2.4 Research gap

Review shown that Muhando, (2018) Conducted Cybersecurity Challenges in African Archives: A Study of Tanzania focusing on inadequate infrastructure and lack of staff training. The study showcased that many archival institutions were vulnerable to cyber-attacks due to outdated systems. and Juma and Kihwele (2021) Conducted Assessing the Impact of Cyber Threats on Information Management: Perspectives from Tanzanian Archives. This research focused on the impact of cyber threats on overall information management within Tanzanian archives. impact of but not the assessment on cyber security threats on management of archives in Tanzania (2026) in bagamoyo.

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

2.6 Conceptual Framework

Independent Variables: which includes Type and frequency of cybersecurity threats (eg., malware, phishing, ransomware), Intervening Variables: which includes Institutional cybersecurity policies and Staff awareness and training and Dependent Variable: and Effectiveness of archives management security

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

CHAPTER THREE

RESEARCH METHODOLOGY

3.0 Introduction

This chapter shows guidelines on how the study was conduct logically or systematically and with observing scientific procedures. It gives details on the nature of the research design, area of the study, population, sample and sampling techniques, ethical considerations and nature of data. Furthermore, it explained the methods that was be used to collect data and how they were analyze to find the answers for respective research objectives.

3.1 Research Design

A mixed-methods approach was be used combining quantitative and qualitative techniques to provide a holistic understanding so by creating a detailed research methodology for a study on the assessment of cybersecurity threats in the management of archives in Tanzania requires consideration of various aspects such as research design, sampling methods, data collection techniques, and analysis strategies. Below is a proposed research methodology for this study, as well as relevant citations to support its components.

This study was employing a 'mixed-methods research design' which combines both quantitative and qualitative approaches. The mixed methods approach facilitates a comprehensive understanding of the cybersecurity threats faced in archive management by combining numerical data with contextual insights (Creswell & Plano Clark, 2017).

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

3.2 Area of the study

Area of the research was be conducted at national archives. Researcher decided to use this area due to geographical area of the study.

3.3 Population of the study

Archive managers, IT personnel, and cybersecurity experts in National archives of Tanzania.

3.4 Targeted population

Refers to the specific group of individuals or entities that the researchers aim to study or gather information from in order to assess the impact of cybersecurity threats on archiving practices within the country. This population is crucial for the research as it informs the validity and applicability of the findings.

Examples of Targeted Population in This Research Context

(a).Archive Managers and Staff, Individuals responsible for the management, preservation, and curation of archives in Tanzania. Their experiences and perspectives on cybersecurity threats can provide valuable insights.

(b)Government Officials: Officials from relevant Tanzanian ministries or agencies overseeing information management, cyber security, and cultural heritage can shed light on policy implications and institutional responses to cyber threats.

(c) IT Professionals, Experts in information technology and cybersecurity who can provide technical assessments of vulnerabilities and potential threats to archival systems.

(d) Researchers and Academics, Scholars studying archives, cybersecurity, or related fields who may have a theoretical interest in the implications of cybersecurity on archival practices.

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

(e) End Users, Individuals or organizations that use archives for research, legal, or cultural purposes; their experiences can highlight the implications of cybersecurity threats on access and usability.

3.5 Sample Size: refers to the selected size of respondents from a large population representing the whole population within the study area (Ran, A. 2020). The sample size was be 25 respondents representing the whole population from the area of study selected. This was including all selected institutional staff from the study area such as records manager, ICT professional, Human resources officer and legal professional so that ensuring a mix of different types of archives for balanced representation (Flick, 2018).

3.6 sampling technique

A sampling technique is a method used to select a portion of a population for study in research. Since studying an entire population can be impractical or impossible, researchers use sampling to gather data from a smaller group that can represent the larger population.

3.6.1 Purposive sampling

Purposive sampling, also known as judgmental sampling, involves selecting individuals based on specific characteristics or criteria relevant to the research. In this method, researchers choose participants who are most likely to provide valuable insights about the topic being studied.

3.6.2 Simple random sampling

Simple random sampling is a technique where every member of the population has an equal chance of being selected. This is usually done using random number generators or

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

drawing lots. The goal is to create a sample that is representative of the whole population, reducing bias and increasing the reliability of results.

3.7 Data Collection Methods

i. Questionnaire

Questionnaires will be administered to archives staff and ICT personnel to collect information about cyber security threats, awareness, existing security measures, and challenges.

ii. Interview

Semi-structured interviews will be conducted with records managers, archivists, ICT officers, and institutional managers to obtain detailed information about cyber security practices and experiences.

iii. Observation

The researcher will observe archive facilities, computer systems, access control mechanisms, backup procedures, and other security measures used to protect archival information.

iv. Document Review

The researcher will review cyber security policies, archives management manuals, ICT security guidelines, audit reports, and institutional records to gather relevant information.

3.7.1 Quantitative data analysis

Blanche (2006) Quantitative data analysis involves transformation of data statistically to assist the researcher in describing the data in a brief and clearly expressed manner. The quantitative data analysis can be used when the data under study can be expressed in form of quantity, number or amount, for instance in terms of mean or averages,

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

frequency and percentage**.** Quantitative data was be coded and analyzed through Microsoft Excel computer program. Descriptive analysis technique was used to reveal the aspects related to the research topic. Quantitative data were presented for each objective in the tables with their frequencies and mean in order to draw conclusion.

3.8 Ethical Consideration

In conducting this study, the researcher paid attention on avoiding plagiarism from various scholars except when dealing with citations and references. The data of this study was be collected by adhering of all procedures required in the whole process of collecting data. The language used is British English; citations relied on American Psychological Association (APA) writing style as per SLADS research guideline. But also, formal language was used by escaping the use of abusive language and the names of respondents were not be mentioned purposeful for maintaining high degree of confidentiality.

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

CHAPTER FOUR

DATA ANALYSIS, PRESENTATION AND DISCUSSION

4.1 Introduction

This chapter presents the data analysis, presentation, discussion, and interpretation of findings of the study on the assessment of cyber security threats affecting the management of archives in Tanzania. The findings are organized according to the four specific objectives of the study. The chapter begins with the questionnaire response rate, followed by demographic details of respondents, and then presents findings based on each research objective.

4.1.1 Questionnaire Response Rate

The study distributed 20 questionnaires to archival staff at the Tanzania National Archives. Out of the 20 questionnaires distributed, 18 were returned and properly completed, indicating a response rate of 90%. In addition, 5 key informants participated in interviews. Therefore, the total number of respondents involved in the study was 23.

A response rate above 70% is considered excellent and sufficient for data analysis in social science research (Creswell & Creswell, 2018). Therefore, the 90% response rate was adequate for reporting and drawing valid conclusions.

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

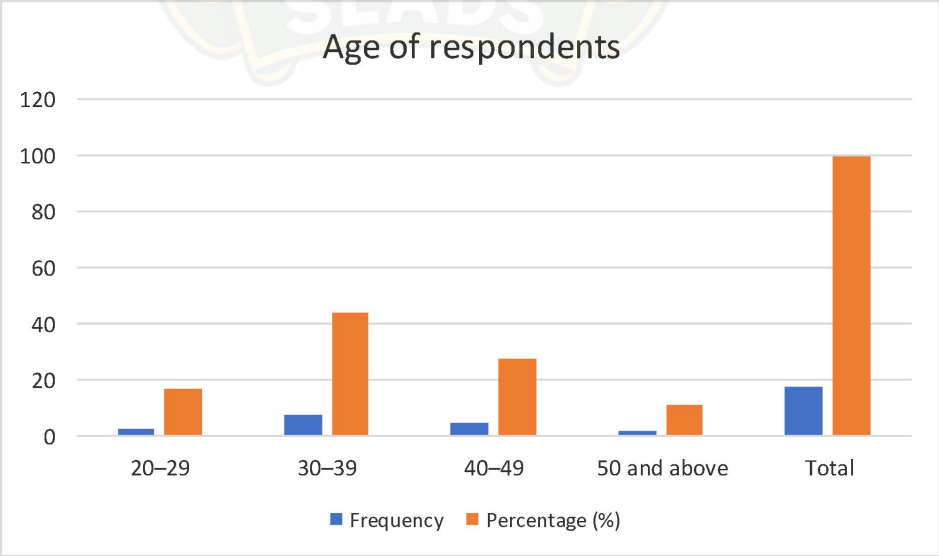
4.2 Respondent's Demographic Details

This section presents the demographic characteristics of the respondents, including age, gender, education level, and position in the institution. Although demographic characteristics were not the main variables of the study, they help in understanding the background of respondents and how such characteristics may influence cyber security awareness and archive management practices.

4.2.1 Respondents Age

The researcher intended to know the respondents' age groups; hence respondents were asked to specify their age categories as it was necessary to understand their age distribution. The respondents were asked to indicate their age because the researcher wished to determine how age characteristics may influence awareness and preparedness in handling cyber security threats in archive management practices.

The results revealed that 8 (44%) respondents were aged between 30–39 years, whereas 5 (28%) respondents were aged between 40–49 years. A total of 3 (17%) respondents were aged between 20–29 years, while 2 (11%) respondents were aged 50 years and above. Moreover, the findings are displayed in Figure 1 below.



SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

Figure 1: Age of Respondents (N = 18)

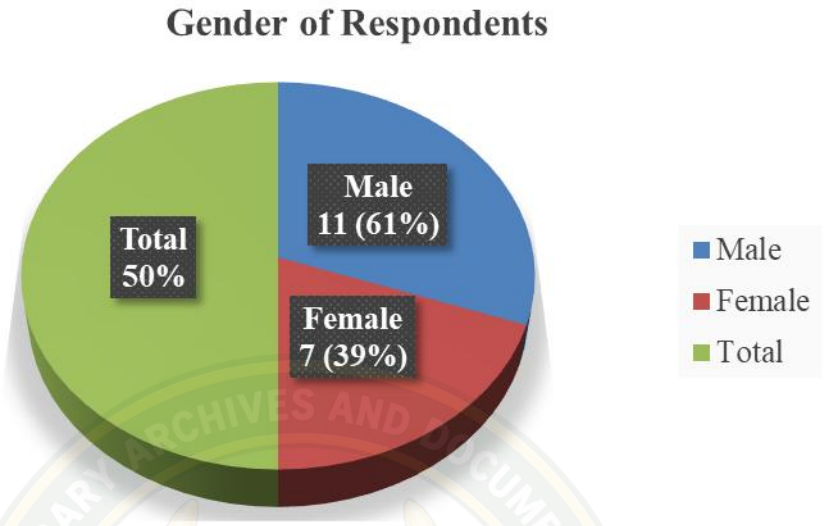
Source: Field Data (2026)

The findings revealed that the majority of respondents were aged between 30–39 years. This indicates that most archival staff are within an active professional age group and are likely to have both practical experience and exposure to digital technologies. Such age distribution suggests that respondents may have adequate experience in archive management while also being adaptable to emerging cyber security practices.

4.2.2 Respondents Gender

In this part, the researcher pursued to know the gender of the respondents so as to detect how gender differences can influence and affect the awareness and management of cyber security threats in archive institutions. Gender diversity is important in ICT and archival professions, as it reflects equal participation in handling digital security responsibilities. The results showed that 11 (61%) respondents were male and 7 (39%) respondents were female. Furthermore, findings are presented in Figure 2 below.

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz



Figuree 2: Gender of Respondents (N = 18)

Source: Field Data (2026)

From Table 2 above, the findings exposed the distribution of the respondents by their gender. The results specified that the majority of respondents were male, while female respondents accounted for a smaller proportion. The findings also revealed that male respondents were slightly more involved in archive and ICT-related duties, which may influence exposure to cyber security awareness and management practices.

On the other hand, the findings show that male respondents represented the largest group engaged in handling archival digital systems. This may be due to the fact that technical and ICT security roles in many institutions are still dominated by male professionals. However, the presence of female respondents indicates that women are also actively participating in archival and digital resource management roles.

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

4.2.3 Education Level of Respondents

Findings of the study indicated that respondents had varying levels of education. The researcher included the level of education because education level may influence understanding, awareness, and ability to manage cyber security threats within archival institutions.

The results revealed that 9 (50%) respondents had a Bachelor's degree, 6 (33%) respondents had a Diploma qualification, while 3 (17%) respondents had postgraduate qualifications. None of the respondents had certificate level only. In more detail, see Figure 3 below.

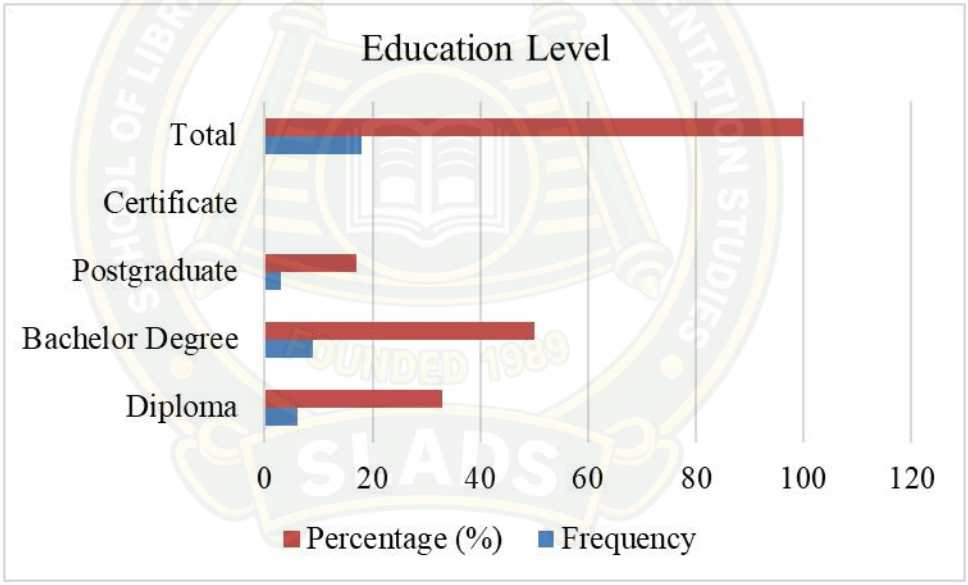


Figure 3: Education Level of Respondents (N = 18)

Source: Field Data (2026)

The findings indicated that the majority of respondents had a Bachelor's degree, followed by those with Diploma qualifications. This implies that most archival staff possess adequate educational background to understand digital systems and cyber

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

security practices. Higher education levels may contribute to better awareness of cyber threats, information security policies, and digital risk management practices.

The results further show that respondents with postgraduate qualifications are relatively few, suggesting the need for advanced professional training in cyber security and digital archives management within Tanzanian archival institutions.

4.2.4 Years of Experience

The respondents were also asked to indicate their years of working experience in archival or ICT-related fields. Experience is an important factor that may influence the understanding and handling of cyber security threats in archive management. The findings are presented in Table 4 below.

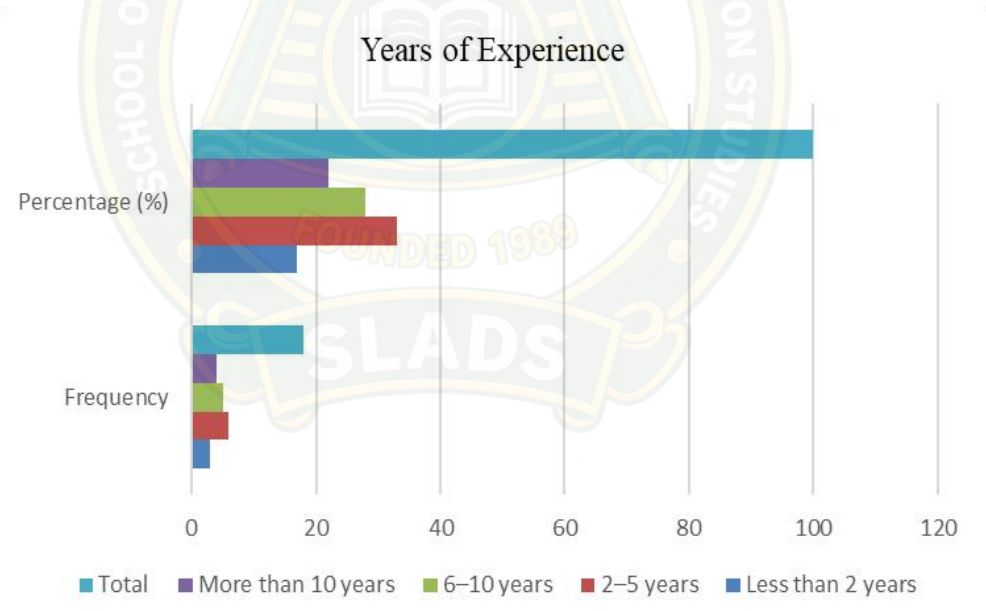


Figure 4: Years of Experience of Respondents (N = 18)

Source: Field Data (2026)

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

The findings reveal that the majority of respondents (33%) had between 2–5 years of experience, followed by 28% who had 6–10 years, and 22% who had more than 10 years of working experience. Only 17% had less than 2 years of experience.

This shows that most respondents had adequate professional experience to understand and respond to cyber security issues in archive management. Such experience is essential for identifying threats, implementing preventive measures, and ensuring compliance with institutional ICT security policies.

4.3 Types of Cyber Security Threats Affecting Archives

Respondents were asked to indicate the type of cyber security threat that has been experienced in their archival institutions. The question aimed to identify the most common threat affecting digital archive management. Respondents were required to choose one main threat experienced in their institution. Five options were provided: malware (viruses, ransomware), phishing attacks, unauthorized access, data breaches, and others.

The collected data as summarized in Table 1 below show that a total of 7 (39%) respondents indicated malware (viruses, ransomware) as the main cyber security threat, 4 (22%) indicated unauthorized access, 3 (17%) indicated phishing attacks, 3 (17%) indicated data breaches, and 1 (6%) indicated other forms of threats.

Table 1: Main Type of Cyber Security Threat Experienced (N = 18)

S/N	Cyber Security Threat	Frequency	Percentage (%)
1	Malware (viruses, ransomware)	7	39
2	Phishing attacks	3	17
3	Unauthorized access	4	22

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

4	Data breaches	3	17
5	Others	1	6
	Total	**18**	**100**

Source: Field Data (2026)

The findings show that malware attacks are the most common cyber security threat affecting archival institutions, followed by unauthorized access. This indicates that many archival systems lack adequate security software, regular system updates, and proper user authentication measures, making them vulnerable to malicious software and unauthorized intrusion. The dominance of malware as the leading threat suggests that basic ICT hygiene practices, such as updating antivirus software, restricting USB usage, and scanning external files, are not consistently applied in archival institutions.

This finding is supported by Mhando (2022), who asserts that malware infections remain a leading cyber security challenge in African archival institutions due to outdated antivirus systems and unsafe data exchange practices. Similarly, Mwanza (2023) argues that unauthorized access is common where institutions do not implement strong password policies and access control mechanisms. The findings further suggest that human factors, such as unsafe computing behavior, may contribute significantly to the spread of malware, indicating the need for staff awareness and training programs.

The researcher also conducted interviews with key informants on the types of cyber threats affecting their archives, and one respondent stated:

> *"The most common problem we face is computer viruses. They come through flash disks and infected email attachments. This has caused loss of some digital records before backup."[Staff Respondent 3, June, 2026]*

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

4.3.1 Frequency of Cyber Security Threats on Archives

Respondents were further asked to indicate how often cyber security threats occur in their archival systems. This question was important because it helps to understand whether cyber threats are occasional, frequent, or rare in archive institutions. Four options were provided to respondents: very often, often, occasionally, and rarely.

The collected data as summarized in Table 2 below show that a total of 8 (44%) respondents selected occasionally, 5 (28%) selected very often, 3 (17%) selected often, and 2 (11%) selected rarely as the frequency at which cyber security threats occur in their archival systems.

Table 2: Frequency of Cyber Security Threats (n = 18)

S/N	Frequency	Frequency (Respondents)	Percentage (%)
1	Very often	5	28
2	Often	3	17
3	Occasionally	8	44
4	Rarely	2	11
	Total	**18**	**100**

Source: Field Data (2026)

The findings reveal that the majority of respondents (44%) indicated that cyber threats occur occasionally, while 28% reported that threats occur very often. This shows that cyber security threats are a regular challenge facing archive institutions in Tanzania, and not just isolated incidents. The fact that only 11% reported that threats rarely occur indicates that virtually all archival institutions are exposed to some level of cyber risk.

This finding is supported by Mwanza (2023), who argues that Tanzanian institutions frequently experience cyber security incidents that disrupt digital operations, although

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

many of these incidents are not formally reported. Similarly, Mhando (2022) notes that the absence of proper monitoring systems makes it difficult to determine the exact frequency of cyber-attacks in many African archival institutions. This suggests that institutions may need to implement formal incident reporting systems to better track and respond to cyber threats.

The researcher also conducted interviews with key informants on the frequency of cyber threats, and one respondent stated:

> *"We experience cyber related problems from time to time. Some months we get several virus alerts, and sometimes staff receive phishing emails. The threats are not constant, but they keep happening throughout the year." [Staff Respondent 1, June, 2026]*

4.3.2 Most Weak Areas of Archival Information to Cyber Threats

Respondents were asked to identify the area of archival information that is most vulnerable to cyber security threats in their institutions. The aim was to determine which part of the archive system is most exposed to cyber risks. Respondents were required to select one area they consider most vulnerable. Five options were provided: digital records, online databases, email systems, backup and storage systems, and others.

The collected data as summarized in Table 3 below show that a total of 7 (39%) respondents indicated digital records as the most vulnerable area, 5 (28%) indicated online databases, 3 (17%) indicated email systems, 2 (11%) indicated backup and storage systems, and 1 (6%) indicated other areas.

Table 3: Most Weak Areas of Archival Information (N = 18)

S/N	Vulnerable Area	Frequency	Percentage (%)

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

1	Digital records	7	39
2	Online databases	5	28
3	Email systems	3	17
4	Backup and storage systems	2	11
5	Others	1	6
	Total	**18**	**100**

Source: Field Data (2026)

The findings show that digital records are the most vulnerable area to cyber security threats, followed by online databases. This indicates that the primary content of archives, the digital records themselves, is the most targeted by cyber threats. This may be due to the fact that digital records are the core assets of archives and therefore the main target for attackers seeking to damage, alter, or steal valuable information.

The vulnerability of online databases (28%) is also significant, as these platforms host searchable catalogs and digital collections that are frequently accessed remotely. This finding is supported by Mwanza (2023), who argues that digital records are the most exposed to cyber risks because they are frequently accessed, shared, and transferred, increasing the chance of interception or corruption. Similarly, Mhando (2022) notes that online databases are highly vulnerable due to weak authentication and limited encryption practices. The lower vulnerability of backup systems (11%) suggests that while backups exist, they may not be sufficiently secured against cyber threats such as ransomware, which can also target backup files.

The researcher also conducted interviews with key informants on the most vulnerable areas in their archival systems, and one respondent stated:

> *"Our digital records are the most at risk because they are stored in computers that are connected to the internet and*

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

shared among staff. If a virus enters one computer, it can easily spread and affect many records."[Staff Respondent 4, June, 2026]

4.4 Existing Cyber Security Measures Used in Archives

Respondents were asked to indicate the main security measure currently in place to protect archival information from cyber security threats in their institutions. The aim was to evaluate the existing protection practices used to safeguard digital archives. Respondents were required to select one main measure used in their institution. Five options were provided: firewalls and antivirus software, regular backups, access control and authentication, staff training programs, and others.

The collected data as summarized in Table 4 below show that a total of 6 (33%) respondents indicated firewalls and antivirus software as the main measure in place, 5 (28%) indicated regular backups, 4 (22%) indicated access control and authentication, 2 (11%) indicated staff training programs, and 1 (6%) indicated other measures.

Table 4: Existing Cyber Security Measures in Archives (N = 18)

S/N	Security Measure	Frequency	Percentage (%)
1	Firewalls and antivirus software	6	33
2	Regular backups	5	28
3	Access control and authentication	4	22
4	Staff training programs	2	11
5	Others	1	6
	Total	**18**	**100**

Source: Field Data (2026)

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

The findings show that firewalls and antivirus software are the most common cyber security measure used in archival institutions, followed by regular backups. This indicates that institutions rely more on technical tools rather than staff training or structured access control systems. While firewalls and antivirus software are important, the limited use of staff training programs (11%) suggests that human capacity development in cyber security is not prioritized.

This finding is supported by Mhando (2022), who asserts that many African archival institutions depend mainly on antivirus software as the first line of defense, while ignoring staff awareness and policy development. Similarly, Mwanza (2023) argues that without proper staff training and access control mechanisms, technical solutions alone cannot fully protect digital archives from cyber threats. This indicates that institutions need to adopt a more balanced approach that combines technical tools with human capacity development and policy frameworks..

The researcher also conducted interviews with key informants regarding the cyber security measures in place, and one respondent stated:

> *"We mainly use antivirus software and we make backups of our records on external hard drives. However, we have never received any formal training on cyber security, and most of us just learn from experience."[Staff Respondent 5, June, 2026]*

4.4.1 Effectiveness of the Existing Cyber Security Measures

Respondents were asked to indicate how effective they consider the existing cyber security measures in safeguarding their archival systems. The aim was to evaluate whether the measures currently in place are sufficient to protect digital records from cyber threats. Four options were provided: very effective, effective, moderately effective, and ineffective.

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

The collected data as summarized in Table 5 below show that a total of 7 (39%) respondents considered the measures moderately effective, 5 (28%) considered them effective, 4 (22%) considered them ineffective, and 2 (11%) considered them very effective.

Table 5: Effectiveness of Existing Cyber Security Measures (N = 18)

S/N	Effectiveness Level	Frequency	Percentage (%)
1	Very effective	2	11
2	Effective	5	28
3	Moderately effective	7	39
4	Ineffective	4	22
	Total	**18**	**100**

Source: Field Data (2026)

The findings show that the majority of respondents (39%) rated the existing measures as moderately effective, while 22% considered them ineffective. This indicates that while some protection exists, the current measures are not considered fully sufficient to safeguard archival systems from cyber threats. The relatively low percentage of "very effective" ratings (11%) suggests that institutions may not have the advanced security infrastructure needed to handle sophisticated cyber threats.

This finding is supported by Mwanza (2023), who asserts that most Tanzanian institutions have basic cyber security measures but lack advanced and comprehensive systems, making their effectiveness only moderate. Similarly, Mhando, (2022) argues that without regular updates, staff training, and proper monitoring, even existing security measures lose their effectiveness over time. This indicates that institutions need to invest in advanced security tools and continuous capacity building to improve the effectiveness of their cyber security measures.

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

4.4.2 Review and Update of Cyber Security Policies

Respondents were asked to indicate how often cyber security policies and measures are reviewed or updated in their archival institutions. The aim was to determine whether institutions regularly maintain and improve their security practices. Four options were provided: monthly, quarterly, annually, and irregularly.

The collected data as summarized in Table 6 below show that a total of 8 (44%) respondents indicated that policies are reviewed irregularly, 5 (28%) indicated annually, 3 (17%) indicated quarterly, and 2 (11%) indicated monthly.

Table 6: Frequency of Review and Update of Cyber Security Policies (n = 18)

S/N	Review Frequency	Frequency (Respondents)	Percentage (%)
1	Monthly	2	11
2	Quarterly	3	17
3	Annually	5	28
4	Irregularly	8	44
	Total	**18**	**100**

Source: Field Data (2026)

The findings show that the majority of respondents (44%) reported that cyber security policies and measures are reviewed irregularly in their institutions. Only 11% indicated that policies are reviewed monthly, while 28% reported annual reviews. This indicates that most archival institutions do not follow a consistent schedule for updating their cyber security measures, which may leave systems exposed to new and evolving threats.

This finding is supported by Mhando, (2022) who argues that many African archival institutions lack proper schedules for reviewing and updating their cyber security policies, resulting in outdated protection measures. Similarly, Mwanza (2023) notes that irregular policy reviews weaken institutional preparedness against emerging cyber threats.

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

4.5 Staff Awareness and Preparedness on Cyber Security

Respondents were asked to indicate whether staff in their institutions are trained on cyber security risks and safe practices for managing archival information. The aim was to assess the level of staff preparedness in dealing with cyber threats in archive management. Four options were provided: yes regularly, occasionally, rarely, and not at all.

The collected data as summarized in Table 7 below show that a total of 9 (50%) respondents indicated that staff are occasionally trained, 4 (22%) indicated rarely, 3 (17%) indicated not at all, and only 2 (11%) indicated that staff are trained regularly.

Table 7: Staff Training on Cyber Security Risks (N = 18)

S/N	Training Frequency	Frequency (Respondents)	Percentage (%)
1	Yes, regularly	2	11
2	Occasionally	9	50
3	Rarely	4	22
4	Not at all	3	17
	Total	**18**	**100**

Source: Field Data (2026)

The findings show that the majority of respondents (50%) reported that staff receive cyber security training only occasionally, while 22% reported that training is rarely conducted. Notably, 17% indicated that staff are not trained at all, and only 11% reported regular training. This indicates that cyber security training in archival institutions is inconsistent and insufficient, which may leave staff unprepared to handle emerging cyber threats.

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

This finding is supported by Mhando (2022) who asserts that many African archival institutions do not have structured cyber security training programs, leaving staff to rely on personal knowledge or experience. Similarly, Mwanza (2023) argues that limited training opportunities are one of the main reasons for poor cyber security preparedness in Tanzanian institutions.

The researcher also conducted interviews with key informants on staff training, and one respondent stated:

> *"We have not had any formal training on cyber security. The only thing we know is from using computers daily. Sometimes our ICT officer gives us small instructions, but there is no proper training program."[Staff Respondent 3, June, 2026]*

4.5.1 Staff Confidence in Handling Cyber Security Incidents

Respondents were asked to indicate how confident they feel in handling potential cyber security incidents affecting archival systems in their institutions. This question aimed to assess the level of preparedness and self-assessed capability among archival staff in responding to cyber threats. Respondents were required to select one option among: Very confident, Confident, moderately confident, and not confident.

The collected data as summarized in Table 8 below show that 4 (22%) respondents indicated that they are very confident, 6 (33%) indicated confident, 5 (28%) indicated moderately confident, and 3 (17%) indicated not confident.

Table 8: Staff Confidence in Handling Cyber Security Incidents (N = 18)

S/N	Level of Confidence	Frequency	Percentage (%)
1	Very confident	4	22
2	Confident	6	33

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

3	Moderately confident	5	28
4	Not confident	3	17
	Total	**18**	**100**

Source: Field Data (2026)

The findings reveal that the majority of respondents (33%) indicated that they are confident in handling cyber security incidents, while 28% indicated moderate confidence. However, 17% reported that they are not confident in responding to cyber threats.

These findings suggest that while some archival staff feel prepared to manage cyber security incidents, a significant proportion may lack sufficient confidence. This may be linked to limited training, inadequate practical exposure to cyber security simulations, or lack of clear institutional response procedures.

According to Ligaya and Semlambo (2024), staff confidence in managing cyber security threats is strongly influenced by the frequency of training and availability of incident response guidelines. Institutions with structured cyber response frameworks tend to demonstrate higher staff confidence levels.

The researcher also conducted interviews with key informants regarding their confidence in handling cyber incidents. One respondent stated:

> *"When minor issues occur, we try to handle them internally, but for major cyber incidents, we depend on external ICT specialists because we are not fully equipped to respond independently." [Staff Respondent 3, June, 2026]*

4.5.2 Clarity of Roles and Responsibilities in Managing Cyber Security Risks

Respondents were asked whether staff in their institution have clear roles and responsibilities in managing cyber security risks affecting archival systems. This

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

question aimed to determine whether institutions have defined accountability structures in handling cyber security matters. Respondents were required to select one option among: Yes, Partially, and No.

The collected data as summarized in Table 9 below show that 7 (39%) respondents indicated that roles and responsibilities are clearly defined, 6 (33%) indicated partially, and 5 (28%) indicated that roles and responsibilities are not clearly defined.

Table 9: Clarity of Roles and Responsibilities in Cyber Security Management (N = 18)

S/N	Response	Frequency	Percentage (%)
1	Yes	7	39
2	Partially	6	33
3	No	5	28
	Total	**18**	**100**

Source: Field Data (2026)

The findings reveal that although 39% of respondents indicated that roles are clearly defined, a combined 61% (partially and no) suggested that clarity is incomplete or lacking. This indicates potential gaps in institutional governance and accountability structures regarding cyber security. Clear assignment of roles is critical for effective incident response, as ambiguity can lead to delays, miscommunication, and increased vulnerability.

According to Ţălu (2025), institutions with well-defined cyber security governance frameworks respond more efficiently to cyber threats and minimize operational disruptions. The findings suggest that some archival institutions in Tanzania may lack formal documentation or communication of cyber security responsibilities, which may

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

delay response and increase vulnerability during cyber incidents. Institutions should therefore develop and communicate clear cyber security responsibility frameworks to all staff.

4.6 Strategies for Improving Cyber Security in Archive Management

The fourth specific objective of this study was to propose a strategic framework for improving cyber security in archive management in Tanzania. Respondents were not directly asked to suggest strategies through the questionnaire; therefore, the findings in this section are drawn from the key informant interviews and supplemented by literature.

During interviews, key informants were asked to suggest possible strategies that could help strengthen cyber security in archive management. The following strategies emerged from their responses:

4.6.1 Regular Staff Training and Awareness Programs

Key informants emphasized that staff are the first line of defense against cyber threats, but many are not adequately trained. They recommended that institutions should organize regular cyber security awareness programs, workshops, and short courses to educate staff on identifying threats such as phishing emails, suspicious links, and unsafe USB devices. Regular training builds a culture of cyber security awareness and reduces human error, which is a leading cause of security breaches (Mhando, 2022)

One interviewee stated:

> *"If we can get training even once or twice a year, it was help us a lot. Many of us do not know how to recognize threats, and that is why our systems get infected easily."[Staff Respondent 2, June, 2026]*

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

This is supported by Mhando (2022) who argues that regular training builds a culture of cyber security awareness and reduces human error, which is a leading cause of security breaches.

4.6.2 Implementation of Strong Access Control and Authentication

Respondents suggested that institutions should strengthen access control by using strong passwords, multi-factor authentication, and restricted user permissions. This ensures that only authorized personnel can access sensitive archival data. Access control mechanisms are essential for protecting digital records from both internal and external threats (Mwanza, 2023). The implementation of these measures should be accompanied by clear policies on password management and user access rights. One interviewee stated:

> *"Right now, many staff use simple passwords and share them. If we can have a system where each person has their own secure login, it was reduced unauthorized access."[Staff Respondent 5, June, 2026]*

This is supported by Mwanza (2023) who asserts that access control mechanisms are essential for protecting digital records from internal and external threats.

4.6.3 Regular Updating of Antivirus Software and Systems

Key informants recommended that institutions should ensure that antivirus software, operating systems, and applications are regularly updated. Outdated systems are highly vulnerable to malware and ransomware attacks. Regular patching and updating of systems is one of the most effective ways of preventing cyber security incidents (Kumar et al., 2017). Institutions should consider implementing automatic update systems to ensure that security patches are applied consistently across all devices.

One interviewee stated:

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

> *"Our computers are not always updated, and sometimes the antivirus expires without us noticing. If the institution can make sure that updates are done automatically, it was helping a lot."[Staff Respondent 1, June, 2026]*

This is supported by Kumar et al. (2017) who argue that regular patching and updating of systems is one of the most effective ways of preventing cyber security incidents.

4.6.4 Development of Institutional Cyber Security Policies

Respondents indicated that their institutions lack formal cyber security policies. They recommended that clear policies should be developed and communicated to all staff. Such policies should cover password management, data backup, incident reporting, and acceptable use of ICT resources. Institutional policies provide a structured framework for cyber security management and ensure consistency in security practices (Mhando, 2022). Policies should be reviewed regularly to remain relevant to evolving threats.

One interviewee stated:

> *"We do not have any written rules about how to handle digital records safely. If the institution can give us a simple policy that we can follow, it was guide us on what to do and what not to do."[Staff Respondent 3, June, 2026]*

This is supported by Mhando (2022) who emphasizes that institutional policies provide a structured framework for cyber security management and ensure consistency in security practices.

4.6.5 Regular Backup of Archival Data

Finally, respondents emphasized the importance of regular and secure backups. They recommended that institutions should implement automatic backup systems and store

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

backup copies in secure offsite locations to ensure recovery in case of data loss or ransomware attacks.

One interviewee stated:

> *"We sometimes make backups, but it is not consistent. If we can have a proper backup schedule and store them safely, we were not fear losing our records." [Staff Respondent 4, June, 2026]*

This is supported by Mwanza (2023) who argues that backup strategies are a critical component of any cyber security framework, particularly for institutions handling irreplaceable records.

4.7 Chapter Summary

This chapter has presented the data analysis, presentation, and discussion of findings based on the four specific objectives of the study. The findings revealed that malware attacks, unauthorized access, and phishing are the most common cyber security threats affecting archives in Tanzania, with digital records being the most vulnerable area. Existing security measures are mainly technical (firewalls, antivirus, backups), but their effectiveness is rated as moderate, and policy reviews are irregular.

Staff awareness and preparedness remain weak, with training being inconsistent and confidence in handling incidents varying. Clear roles and responsibilities are not fully defined in many institutions. The study proposed five key strategies: regular training, strong access control, system updates, policy development, and consistent backups.

Overall, the findings indicate that while some cyber security measures exist in Tanzanian archival institutions, significant gaps remain in training, policy frameworks, and institutional governance. A comprehensive approach combining technical, human, and policy interventions is required to strengthen cyber security in archive management.

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

CHAPTER FIVE

SUMMARY, CONCLUSION, AND RECOMMENDATIONS

5.0 Introduction

This chapter presents a summary of the findings, conclusion, and recommendations based on the data collected and analysed in Chapter Four. The chapter concludes by

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

proposing areas for further research related to cyber security threats affecting archive management in Tanzania.

5.1 Summary of the Findings

The study was conducted at the Tanzania National Archives. The study focused on the assessment of cyber security threats affecting the management of archives in Tanzania. The study involved 23 participants, where 18 respondents completed questionnaires and 5 key informants participated in interviews. The study was guided by four specific objectives and four research questions. Respondents' demographic characteristics were recorded, including age, gender, education level, and years of experience. The majority of respondents were aged between 30–39 years (44%), followed by those aged 40–49 years (28%). The findings also revealed that 61% of respondents were male and 39% were female. In terms of education level, 50% of respondents had a Bachelor's degree, 33% had Diploma qualifications, and 17% had postgraduate qualifications. Most respondents had between 2–5 years of working experience (33%).

The first specific objective was to identify the main types of cyber security threats affecting archives in Tanzania. The findings revealed that malware (39%) was the most common cyber security threat experienced in archival institutions, followed by unauthorized access (22%). Additionally, the majority of respondents (44%) indicated that cyber security threats occur occasionally, while digital records (39%) were identified as the most vulnerable area to cyber attacks.

The second specific objective was to evaluate current practices and institutional measures for safeguarding archives against cyber threats. The findings showed that firewalls and antivirus software (33%) were the most commonly used security measures, followed by regular backups (28%). However, most respondents rated these measures as moderately effective (39%). Furthermore, 44% of respondents reported that cyber

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

security policies are reviewed irregularly, indicating weak institutional monitoring and updating mechanisms.

The third specific objective was to assess staff awareness and preparedness in managing cyber security risks. The findings showed that staff training on cyber security is conducted only occasionally (50%), and 22% indicated that training is rarely conducted. While 33% of respondents reported being confident in handling cyber incidents, 17% indicated lack of confidence. Additionally, 61% of respondents reported that roles and responsibilities in managing cyber security risks are either partially defined or not clearly defined.

The fourth specific objective was to propose strategies for improving cyber security in archive management. Based on interview findings, key strategies identified include regular staff training programs, strengthening access control mechanisms, regular system updates, development of formal cyber security policies, and implementation of structured data backup systems.

5.2 Conclusion

Based on the findings of this study, it can be concluded that archival institutions in Tanzania are exposed to various cyber security threats, particularly malware and unauthorized access. While basic protective measures such as antivirus software and firewalls are in place, their effectiveness is only moderate due to irregular policy review, limited staff training, and unclear assignment of cyber security responsibilities.

The study also concludes that staff preparedness remains inadequate, as training programs are inconsistent and confidence levels vary among staff members. Furthermore, the lack of structured institutional cyber security policies increases the vulnerability of archival systems.

Therefore, without strengthening technical infrastructure, improving staff training, and establishing clear cyber security governance frameworks, archival institutions in

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

Tanzania was remain at risk of cyber threats that may compromise the confidentiality, integrity, and availability of archival records.

5.3 Recommendations

Based on the findings of this study, the following recommendations are proposed:

First, archival institutions should implement regular and structured cyber security training programs for all staff. Continuous training was improved awareness, reduce human error, and enhance preparedness in handling cyber threats.

Second, institutions should strengthen access control mechanisms by introducing strong password policies, multi-factor authentication, and user access restrictions to prevent unauthorized access.

Third, there should be regular updating of antivirus software, operating systems, and archival management systems to prevent exploitation of system vulnerabilities.

Fourth, institutions should develop and implement formal cyber security policies that clearly define staff roles, incident response procedures, password management guidelines, and data protection measures.

Fifth, archival institutions should establish structured and automated backup systems, including secure off-site backups, to ensure recovery of records in case of cyber incidents such as ransomware attacks.

Finally, government authorities should allocate sufficient budgetary support to archival institutions to strengthen cyber security infrastructure and provide modern digital protection tools.

5.4 Recommendations for Further Studies

- The researcher proposes that future studies on this topic should focus on the following areas:

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

- A comparative study of cyber security threats in public and private archival institutions in Tanzania.
- An assessment of the effectiveness of national cyber security policies in protecting digital archives.
- Investigation of the impact of cyber security breaches on public trust in archival institutions.
- A study on advanced cyber security frameworks suitable for digital preservation systems in Tanzania.

REFERENCES

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

Chimwaga, C. (2022). Cybersecurity in Cultural Institutions: Challenges and Solutions*. Journal of Information Studies, 10(2), 45-60.

Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approach (5th ed.). SAGE Publications.

Dillman, D. A., Smyth, J. D., & Christian, L. M. (2014). Internet, phone, mail, and mixed-mode surveys: The tailored design method (4th ed.). Wiley.

International Telecommunication Union (ITU). (2023)."Cybersecurity Frameworks for Digital Content Management in Developing Countries."

Jones, R., & Smith, L. (2022). "Securing Digital Archives Against Cyber Threats: Lessons from Emerging Economies." Cybersecurity Review, 8(3), 110-126.

Khan, A., Jamil, F., & Ali, M. (2022). Cybersecurity in Archives: Challenges and Solutions. *Journal of Archival Science, 12*(3), 245-260.

Kihwele, N. M., & Sanga, C. (2023)."Digital Archives and Cybersecurity Risks in Sub-Saharan Africa: A Case Study of Tanzania." International Journal of Digital Preservation, 17(1), 34-50.

Kumar, R., Prakash, R., & Kumar, L. (2017). Understanding Cyber Security Threats in Archives and Records Management. International Journal of Information Management, 37(2), 118-126.

Ligaya, R. S., & Semlambo, A. A. (2024). Safeguarding digital frontiers: cybersecurity threat mitigation in Tanzanian local governments. African Conference of Applied Informatics.

Ligaya, R. S., & Semlambo, A. A. (2024). Safeguarding digital frontiers: Cybersecurity threat mitigation in Tanzanian local governments. African Conference of Applied Informatics Proceedings.

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

Mhando, J. (2022). Current State and Future Directions of Archival Science in Tanzania*. Archives and Records Management, 9(1), 35-50.

Mhando, J. (2022). Current state and future directions of archival science in Tanzania. Archives and Records Management Journal, 9(1), 35–50.

Moyana, N. S., & Chuma, K. G. (2023). Cybersecurity of information systems at the National Archives and Records Service of South Africa. South African Journal of Libraries and Information Science.

Mwanza, R. (2023). The Impact of Cyber Threats on Historical Archives: A Tanzanian Perspective. International Journal of Cybersecurity, 15(1), 23-4

Mwanza, R. (2023). The impact of cyber threats on historical archives: A Tanzanian perspective. International Journal of Cybersecurity Studies, 15(1), 23–40.

Ndung'u, T., & Wainaina, G. (2020). Challenges in digital record-keeping and cybersecurity in Tanzanian government agencies. African Journal of Information Systems, 12(4), 78–89.

Ndung'u, T., & Wainaina, G. (2020)."Challenges in Digital Record-Keeping and Cybersecurity in Tanzanian Government Agencies." African Journal of Information Systems, 12(4), 78-89.

Semlambo, A., & Shalua, N. S. (2024). Assessing Cybersecurity Threats to Tanzania's gyGovernment E-Payment Systems and Their Impact on National Security. The Journal of Informatics.

Ţălu, M. (2025). Cyberattacks and Cybersecurity: Concepts, challenges, and future research. Digital Technologies Research and Applications.

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

Ţălu, M. (2025). Cyberattacks and cybersecurity: Concepts, challenges, and future research directions. Digital Technologies Research and Applications, 3(2), 101–115.

Tanzania Cybercrimes Act of 2015.

Tanzania National Archives. (2020)."Annual Report on Digital Data Security.

UNESCO. (2021). Guidelines for Digital Archives Management in Africa. UNESCO Publication.

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

APPENDIX I

RESEARCH QUESTIONNAIRE

Dear respondents,

I am **DEVIS M. SINKALA** a student of SLADS pursuing Diploma in Records and Archives Management. Currently I am conducting a research project titled "***Assessment of Cyber Security Threats on Management of Archives in Tanzania".***

I was highly appreciating your cooperation in filling this questionnaire, which was take not more than 20 minutes. All information provided was be kept confidential and only used for the purpose of the study.

Please tick (✓) or fill where appropriate:

1. Gender:
   a) Male ( )
   b) Female ( )
   c) Other ( )
2. Age:
   a) 18–25 ( )
   b) 26–35 ( )
   c) 36–45 ( )
   d) 46 and above ( )
3. Education Level:
   a) Certificate ( )
   b) Diploma ( )
   c) Degree ( )
   d) Postgraduate ( )
4. Position in Institution: _____

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

5. Years of Experience in Records/Archives Management:
   a) Less than 1 year ( )
   b) 1–3 years ( )
   c) 4–6 years ( )
   d) 7 years and above ( )
6. What types of cyber security threats has your institution experienced in relation to archival systems?
   a) Malware (viruses, ransomware) ( )
   b) Phishing attacks ( )
   c) Unauthorized access ( )
   d) Data breaches ( )
   e) Others (please specify) _____
7. How frequently do cyber threats occur in your archival system?
   a) Very often ( )
   b) Often ( )
   c) Occasionally ( )
   d) Rarely ( )
8. Which areas of archival information are most vulnerable to cyber threats?
   a) Digital records ( )
   b) Online databases ( )
   c) Email systems ( )
   d) Backup and storage systems ( )
   e) Others (please specify) _____
9. What measures are currently in place to protect archival information from cyber threats?
   a) Firewalls and antivirus software ( )
   b) Regular backups ( )
   c) Access control and authentication ( )

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

d) Staff training programs ( )

e) Others (please specify) _____

10. How effective do you think these measures are in safeguarding archival systems?

a) Very effective ( )

b) Effective ( )

c) Moderately effective ( )

d) Ineffective ( )

11. How often are cyber security policies and measures reviewed or updated?

a) Monthly ( )

b) Quarterly ( )

c) Annually ( )

d) Irregularly ( )

12. Are staff trained on cyber security risks and safe practices for managing archival information?

a) Yes, regularly ( )

b) Occasionally ( )

c) Rarely ( )

d) Not at all ( )

13. How confident are you in handling potential cyber security incidents affecting archival systems?

a) Very confident ( )

b) Confident ( )

c) Moderately confident ( )

d) Not confident ( )

14. Do staff have clear roles and responsibilities in managing cyber security risks?

a) Yes ( )

b) Partially ( )

c) No ( )

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

APPENDIX II

INTERVIEW GUIDE

Interview Guide for Administrative Staff

1. Can you describe the main cyber threats that have affected your archival systems in recent years?
2. Which systems or types of archival data are most vulnerable to cyber threats, and why?
3. How has your institution responded to past cyber security incidents affecting archives?
4. What formal measures, policies, or protocols does your institution have to safeguard archival information from cyber threats?
5. How often are these measures reviewed, and how effective have they been in practice?
6. What challenges do you face in implementing or maintaining these security measures?
7. How would you assess staff awareness and understanding of cyber security in your institution?
8. What training or support is provided to staff for managing cyber security risks?
9. How prepared do you think staff are to respond to cyber security incidents affecting archival information?

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

APPENDIX I REAEARCH WORK PLAN/ SCHEDULE TIME FRAME

The research was be conducted for the period of six (6) weeks as follow

ACTIVITIES PROGRAM	**1ST WEEK**	**2ND WEEK**	**3RD WEEK**	**4TH WEEK**	**5TH WEEK**	**6TH WEEK**
Reporting at the working place						
Familiarization and distribution of questionnaire						
Interview Schedules						
Collection of data and compilation						
Data analysis and presentation						
First draft proof reading and final report submission						

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

APPENDIX II

BUDGET

The study was required money in order to achieve the goals for data collection. It includes stationery, transport expenses as well as daily expenses for researcher survival. The expenditure was be as the follow:

S/N	Item	Quantity	Cost
1	Pens	1box	8,000/=
2	Papers	1ream @ 15000	15,000/=
3	Questionnaire and interviews questions preparation	50 copies @ 200	10,000/=
4	Typing and printing proposal		45,000/=
6	Meals	45 days @ 5000	225,000/=
	TOTAL		**338,000/=**

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

APPENDIX III

APPROVAL LETTER

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz

THE UNITED REPUBLIC OF TANZANIA

PRESIDENT'S OFFICE
RECORDS AND ARCHIVES MANAGEMENT DEPARTMENT

Telephone: (+255) 26 2963135
Email: ramd@nyaraka.go.tz

In reply please quote:
Ref. No. BA. 18/203/01B/36

6 Swaswa Road,
P.O. Box 2316,
DODOMA.

12th May, 2026

Academic Officer,
Tanzania Library Services Board,
School of Library, Archives and Documentation Studies,
P.O. Box 227,
PWANI.

Re: **STUDENTS INTRODUCTION FOR RESEARCH WORK**

Please refer your letter with Ref. No. 201/457/VOL/1/20 of 29th April, 2026 regarding subject above.

2. The Department is pleased to inform you that, **Mr. Devis Malius Sinkala** has been granted permission to collect data regarding his research title ***"Assessment of cyber security threat on Management of Archives in Tanzania: Case study in National Archives"*** as requested.

Thank you for your continued cooperation.

Firimin M. Msiangi
DIRECTOR
RECORDS AND ARCHIVES MANAGEMENT DEPARTMENT

SLADS Research Hub · SLADS/2026/00073 · repository.slads.sc.tz