

**ASSESSMENT OF THE EFFECTIVENESS OF NON-TECHNICAL APPROACH
TO CYBER SECURITY MANAGEMENT FOR KENYA MINISTRY OF LANDS
AND PHYSICAL PLANNING NLIMS SYSTEM.**

GABRIEL NDUNG’U

**A Research Thesis Submitted to School of Computer Science in the Partial
Fulfilment for the Degree Master of Science Computer Information System at
Kenya Methodist University**

OCTOBER, 2024

DECLARATION AND RECOMMENDATION

Declaration:

I, Gabriel Ndung'u the undersigned, declare that this thesis is a product of my own work and it has not been previously presented to any other institution. All sources have been appropriately cited and duly acknowledged in full.

I consent that this thesis may be available for reference and photocopying at the discretion of the University.

Student: Gabriel Ndung'u

Admission Number: CIS-3-2653-2/2014

Signature.....

Date:

Approval:

I approve/disapprove that this is/is not' the original work of the above author as the research supervisor for Kenya Methodist University Nairobi, Campus.

Supervisor 1: Dr. Lawrence Mwenda

Signature:

Date.....

Supervisor 2: Mr. Robert Murungi

Signature:

Date.....

COPYRIGHT
© 2024 Gabriel Ndung'u

All rights reserved. No part of this document may be reproduced, stored in any retrieval system or transmitted in any form or by any means, electronically, mechanically, by photocopying or otherwise, without prior written permission of the author or Kenya Methodist University, on that behalf

DEDICATION

I dedicate this thesis to my beloved wife, Juliet Maina, my cherished daughter, Zariah Wambui Ndung'u, and my dear son, Nathan Njuguna Ndung'u. Their unwavering support, encouragement, and love has been my greatest source of strength throughout the entire research journey.

ACKNOWLEDGEMENT

I am most grateful to God, for successfully taking me through the whole masters degree course. My appreciation go to my supervisors Dr. Lawrence Mwenda and Mr. Robert Murungi, for their academic guidance, support, encouragement, inspiration, and for giving me their time expert knowledge and wisdom. I am also indebted to my My Wife Juliet Maina, children Zariah Wambui and Nathan Njuguna for their understanding, encouragement and understanding throughout my study.

I am also grateful of the support that I got from all the Kenya Ministry of Lands and Physical Planning during data collection. I further acknowledge heads of ICT of NLIMS for accepting to participate in my study by filling the questionnaires. I am also thankful to all my research assistants for their hard work.

I also wish to thank fellow masters students of Kenya Methodist University for being good comrades throughout the time I was doing my study. I also appreciate faculty members for their insights and advice for my research. Finally, I wish to thank my colleagues in the land ministry department and friends for their encouragement and support throughout the study.

ABSTRACT

Cyber security threats and vulnerabilities are influenced by human behavior, making them complex systems. The conventional reductionist approach to managing technical aspects of cyber security is limited, as it cannot predict the non-technical aspects of cyber security. The complexity approach, however, offers a robust and effective way to predict social aspects of cyber security. This study aims to assess the effectiveness of the Ministry of Land's approach to non-technical cyber threats and vulnerabilities. Current studies focus predominantly on the technical aspect cyber security and less on social aspect of cyber security at the detriment of the social side so does the setup and implementation of information security system. In aggregate system that focus on the technical side are weak on the social aspect and predisposed to social-engineering attack, Data will be collected through face-to-face interviews with Ministry of land staff linked to the NLIMS system in Nairobi. The findings indicate that at least 70% of staff lack knowledge of social engineering attacks, their conduct, and skills to prevent or stop them. Lower-rank staff access information they are not authorized to access through the workstation resource sharing policy. The study reveals that KMLPP's non-technical approach to cyber security is ineffective in protecting sensitive information and preventing staff from accessing sensitive data through dumb star diving. It also highlights the vulnerability of lower-rank staff to shoulder surfing and workstation privacy exploits. The study proposes a socio-technical cybernetic enterprise model, which focuses on staff relationships and restricts information access without appropriate privileges, ensuring a more secure environment for NLIMS.

TABLE OF CONTENTS

CONTENTS	
DECLARATION AND RECOMMENDATION	ii
COPYRIGHT	iii
DEDICATION	iv
ACKNOWLEDGEMENT	v
ABSTRACT	vi
TABLE OF CONTENTS	vii
LIST OF TABLES	ix
LIST OF FIGURES	x
LIST OF ABBREVIATIONS & ACRONYMS	1
CHAPTER ONE	2
INTRODUCTION	2
1.1 Background information	2
1.2 Statement of the Problem	14
1.3 Objective of the Study	15
1.4 Justification of the Study	16
1.5 Assumptions of the Study	17
1.6 Limitations of the Study	17
1.7 Scope and Delimitations of the Study	17
1.8 Organization of the Study	17
CHAPTER TWO	19
LITERATURE REVIEW	19
2.1 Introduction	19
2.2 Information Security	19
2.3 Information Security Threats	21
2.4 Theoretical Framework	24
2.5 Empirical Literature Review	31
2.6 Conceptual Framework	37
2.7 Research Gaps	37
2.8 Summary of the Chapter	38
CHAPTER THREE	40
RESEARCH METHODOLOGY	40
3.1 Introduction	40

3.2 Location of the Study	40
3.3 Research Design.....	40
3.4 Target Population and Sample Selection Procedures.....	41
3.5 Data Collection Instruments.....	42
3.6 Data Processing and Analysis Procedures	44
3.7 Piloting of Research Instruments	44
3.8 Validity of Research Instruments.....	44
3.9 Reliability of Research Instruments	45
3.10 Summary of Research Objectives, Hypotheses, and Analytical Models-100.....	45
3.11 Operationalization of Study Variables	46
3.12 Ethical Considerations.....	47
3.13 Summary of the Chapter	48
CHAPTER FOUR.....	49
RESULTS AND DISCUSSION	49
4.1 Introduction	49
4.2 The Study's Response Rate.....	49
4.3 Summary of the Study Results	49
4.4 Data Analysis	61
4.5 Summary	65
4.6 Discussion of the Findings	66
CHAPTER FIVE	71
SUMMARY, CONCLUSION AND RECOMMENDATIONS	71
5.1 Summary	71
5.2 Conclusions	72
5.3 Recommendations	73
5.4 Implications for Further studies	75
REFERENCES.....	76
APPENDICES	85

LIST OF TABLES

Table 4. 1 Printed document waste disposal	50
Table 4. 2 Electronic storage waste disposal.....	51
Table 4. 3 Optical storage waste disposal	53
Table 4. 4 How should surfing occur in the workplace and home	54
Table 4. 5 Workstation resource sharing.....	56
Table 4. 6 Social engineering awareness test sample size 40	58
Table 4. 7 T- test table derived from table 4.6	62
Table 4. 8 Descriptive statistical analysis of shoulder surfaces	63
Table 4. 9 T-test panel significance level of .05 or 5%.....	64
Table 4. 10 Workstation resource sharing sample size 40 respondents	65

LIST OF FIGURES

Figure 2. 1 A socio-technical cybernetic enterprise model.....	28
Figure 2. 2 Responsibility dependency	30
Figure 2. 3 Diagram indicating the interaction of variables	37
Figure 4. 1 Printed document waste disposal.....	51
Figure 4. 2 Electroni storage waste disposal.....	52
Figure 4. 3 Optical storage waste disposal.....	53
Figure 4. 4 How shoulder surfing occurs in the workplace and home.....	55
Figure 4.5 Station privacy: shoulder surfing by percentage.....	56
Figure 4. 6 Working station resouces shared by percentage.....	57
Figure 4. 7 Social engineering awarenness test sample size 40.....	59
Figure 4. 8 Social awareness test sample size 40 response sumamary	60
Figure 4. 9 Social engineering awarenss test sample size 40 section B.....	60
Figure 4. 10 Social engineering awarenes test sample size 40 section B response summary.....	61
Figure 4. 11 A socio-technical cybernetic enterprise model	62

LIST OF ABBREVIATIONS & ACRONYMS

NLIMS: National Lands Information Management System. An information infrastructure used by the ministry of lands of Kenya to store, organize land registration records.

SCADA: Supervisory Control and Data Acquisition. This is a software type of an information system that is used in controlling industrial process. It gathers data from remote site and control the infrastructure example traffic system.

ICT: Information Communication Technology. A composite term used to describe information infrastructures such as NLIMS, SCADA and other alike.

ABM: Agent Based Modelling. An approach to non-technical cyber security based on complexity theory.

STS: Social-technical system. An information security approach that takes into account the hardware, software, personal, and community component of a system designed for a particular purpose (Norman, 2022)

KMLPP: Kenya Ministry of Lands and Physical Planning. A Kenya Government parastatal that conducts land registration, transfer and physical planning.

CHAPTER ONE

INTRODUCTION

Introduction

This chapter's subtopics include background information regarding the research issue, problem statement, research aims and questions, study rationale, and importance. It closes with the study assumptions, research scope and delimitation, study limitations, and term definitions.

1.1 Background information

This study conducts an assessment of the effectiveness of a non-technical approach to cyber security management for Kenya's Ministry of Lands and Physical Planning NLIMS system. This seeks to collect data on the current state of security measures employed to mitigate the weaknesses that are associated with the social aspect of the information system in matters of cyber security in critical information infrastructure such as SCADA and for the case of this thesis NLIMS.

1.1.1 National Lands Information Management System

According to the Ministry of Lands and Physical Planning (MLPP) in Kenya, system digitization was among the four priorities spearheaded in the ended financial year 2019/2020. Now the digitization process is in its pilot phase in the Nairobi region. The conceptualization of this paper considers the fact that the nature and framework of the new NLIMS used in the Ministry of Lands and Physical Planning is not accurately known. The intended purpose is understood as outlined by the ministry as follows; to enhance the

security of land records, improve accessibility, cut down land transaction costs, enhance transparency, and promote paperless transactions (MLPP, 2021).

This system is intended to bring much and long-awaited changes to the land registry. Considering the advanced nature of cyber threats, information security is of key importance in any ICT-based system especially one that handles bulk information transactions nationwide. A system is as secure as its last security patch, therefore, to improve cyber security nations have embraced global collaboration in information sharing pertaining to security threats. It is apparent that the developers of the NLIMS had security in mind, but its ability to match global standards and leverage current technology is the matter in question here. The most valuable resource that the NLIMS handles is the information on land transactions in the form of land records. The security of this information is affected by the application security, network security, end-users, and operation security among other factors.

In an information security framework, two parts are a subject of concern, when designing deterrence approaches and analyzing failures. The technical part deals with hardware and software infrastructure and the non-technical or sociotechnical part. Hamid Salim states that,

“Existing cyber security approaches mostly focus on technical aspects, to create a secure 2 fence around technology assets of an organization. This limits systemic thinking for three main reasons: First, it does not view cyber security holistically at an organizational level, which includes people and processes. Second, the focus on security technology reinforces the perception that it is solely an Information Technology department problem. Third, within the context of the cyber ecosystem, focusing only on a technical solution ignores

interactions with other systems/sub-systems operating beyond an organizational boundary” (Salim & Madnick, 2016).

As emphasized by Savage (2009) and Hamid (2016) cyber security is a holistic attribute of an information system rather than just one of its elements. This study builds on Hamid's worries about people's roles in information system security. This study focuses on the non-technical aspects of the NLIMS.

The complexity and ingenuity that go into the instigation of the current cyberattacks have perpetually taken world cyber security operations by surprise hence no system is secure from future attacks. Kioskli and Polemi (2020) discuss the use of a socio-technical approach in threat assessment by delving into the attacker's behavioural psychology. The nature of cyber security today has been made complex by non-technical vulnerabilities that are brought about by human behaviour (Gandhi, 2014). There is a need for a comprehensive strategy for cyber security in which non-technical threats and weaknesses are adequately addressed.

A conventional reductionist approach to non-technical threats is limited by the ability of the threat or vulnerability to evolve and adapt to the environment. This makes it hard to anticipate attacks or even identify weaknesses.

1.1.2 Government ICT/ information system

Government ICT/information, also known as E-government, is when government departments, ministries, and parastatals use ICT infrastructure such as the web, and handheld devices to change operations with citizens and businesses. There are several avenues that the said technologies provide utility. Some of the most common tasks accomplished are the consolidation of various government services to citizens under one

system, place, or platform for easy accessibility example 'HUDUMA CENTRE'. Secondly, the technologies can also improve the interactions with business and industry. The advent of the use of E-government has brought about a reduction in graft cases, augmented government transparency level, and there has been a tremendous increase in convenience in access and dispensation of government service. World Bank (2011) has also reported that e-government has brought about revenue growth, and operation cost reductions (Lukorito, 2012).

In Kenya practically, all ministries and departments have an information system, some are independent and there are those that are not. For example, the Kenya Energy Petroleum Regulation Authority- KEPRA, the Ministry of Lands, Kenya Revenue Authority are some of the many large departments that have independent systems. These systems store critical personal Identifiable information, accounts, and e-commerce systems that transact hundreds of millions per day. The operations that are conducted with these systems transform people's lives and as such they will attract the attention of criminals. Some of these systems have been attacked before and a substantial amount of money was lost and some recovered, for example, KRA (Lukorito, 2012).

The Advent of attacks on e-government platforms has led to the strengthening of the technical part of the information system. The human part is rather difficult since consistent adherence to security policies is elusive, especially for low-ranking employees (Lukorito, 2012). Low-ranking employees tend to possess less technical knowledge about cybercrime because of their academic qualification or the nature of their role which in most cases is not technical or Information system related. With such attributes the low-ranking employees become the primary target of social engineering, a cybercrime tactic to gather

information from a subject for potential cyber-attack. Human behavior is not as predictable as a technical system and even an employee who strictly adheres to information system security policies to some degree can assume that there will be a situation whereby such an individual will fail to comply, for example, if there is a threat to their life.

1.1.3 Information Security Threats

An information security threat is defined as any condition or occurrence that has the potential to cause damage to an information system through unlawful access, data destruction, disclosure, alteration, and/or denial of service (Yang, 2008). Hacking is a prevalent danger that involves breaking into a computer system to gain unauthorized access by evading its security measures (Chandler, 1996). The attack known as denial-of-service (DOS) is a distinct type of threat in which an attacker overwhelms a server or network with meaningless orders, draining its resources and making the service inaccessible (Alfawaz et al., 2008). There is also the threat of spam. Spamming is the practice of sending unwanted bulk communications to a large number of people at once, sometimes thousands, with the primary objective of marketing items to potential customers, Chandler (1996) explained. Malware attacks are an extra concern. Malware is delivered in a variety of ways, including worms sent over email and SMS, Trojan horses downloaded from websites, and virus-infected files obtained via internet connections. They could also be the consequence of mobile devices that are linked to computers, thumb drives, and compact disks—all of which are removable media (Yang, 2008). Threats might also emerge from software flaws. A computer program or system fault is described as an error, defect, mistake, failure, or fault that generates an inaccurate or unexpected conclusion or leads it to act in an unforeseen manner (Yang, 2008). Users with too many privileges might likewise represent

a problem. Users should be provided just the necessary permissions to carry out their obligations.

1.1.4 Cybercrime

The term "cybercrime" refers to any act during which a computing device or communication networks are utilized as a weaponized, designated as a target, or made a premise for criminal conduct. While the word "cybercrime" is often used to describe criminal conduct in which a computer or network is a key component, it can be delimited to apply to more traditional crimes in which unlawful activity is made feasible by the use of computers or networks (Forde & Patterson, 2003). The Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (Vienna, 2000) classified five offenses as cybercrime: illicit access, destruction to computing hardware, information, or applications, tampering that hinders an ICT infrastructure from working, and unapproved interception of information to, from, and within a computer spying, system, or network (Forde & Patterson, 2003). Device abuse, forgery (identity theft), digital fraud, data disruption (unapproved damage, erasure, degradation, modification, or inhibition of electronic data), and systems disruption (disrupting the functioning of a computer system through entering, transmitting, damaging, deleting, weakening modifying, or inhibiting computer data)

The convergence of computing and communications has resulted in remarkable current and future technological advancements that have already profoundly impacted many facets of daily life. Air traffic, stock exchanges, and banks Information technology and telecommunications are essential to the operation of many different types of institutions related to health, welfare, and education, as well as control, telephones, and electric power.

The speed at which the modern world is developing allows one to claim that computer software is the basis for everything. Technology's exponential growth, capacity and accessibility gains, and cost reductions have resulted in revolutionary changes in the areas of crime, communications, entertainment, and commerce (Grant & Grabosky, 1997).

But greater vulnerability also comes with this greater capacity. With the use of information technology, criminals can now conduct crimes from the comfort of their desks. As Kenya's electronic commerce volume continues to rise, so does the number of people with Internet connections. Approximately Along with the world's increasing size comes increased connectivity, raising both the number of potential offenders and victims of computer-related crime (Grabosky, 2000). Several sorts of unlawful activities may be perpetrated using or against information technology. Some of them are just innovative in form; the content is not. Others advocate for whole new forms of illegality. In national capitals, there is a growing awareness of the threat posed by crimes against computers or computer-related information. There are laws against these kinds of crimes that are probably unenforceable in the majority of the world's nations. Businesses and governments are forced to rely entirely on technological measures to protect themselves due to this lack of legal protection from those who steal, obstruct, or destroy important data.

1.1.5 Employees compliance with the Information Security Policy

The management of information security in firms or organizations has been and still is a daunting endeavor, particularly trying to avoid the threats and risks from within the firm. Studies have shown that employee carelessness and those who are deviant constitute a key threat to organizations' cyber security threat (Mikko et al., 2007). Every organization has an information security policy that is meant to help mitigate information security risks

posed by the employees. It is also true that not all employees are willing to strictly comply with such policies (Stanton et al., 2005).

Literature also indicates a tremendous failure of such policies to influence employee behavior toward compliance (Puhakainen, 2006; Siponen, 2000). Studies also indicate a great deviation in behavior from country to country about the compliance behavior of the employees towards the cyber security policies (Hovav & D'Arcy, 2012). As such it is a poor foundation to approach the construction of security policies based on behavioral studies of a different country. There are a lot of factors that come into play toward the overall influence of employee behavior on compliance with information security policies. In the case, of Kenya, we have factors such as; cyber security knowledge gap, ethics, proliferation of technology, and e-waste disposal infrastructure (Sang et al., 2014).

In Kenya every potential employee is mandated to at least have undertaken a certificate course in computer fundamentals. The course basically constitutes Microsoft software suite (MS. Word, Excel, Publisher, Powerpoint, and Access), internet and email, and Adobe Page. The course does not cover information security or fundamentals of cyber security. Therefore, most employees lack critical knowledge in cyber security when they get hired save for the IT employees (Raphael et al., 2023). Such a knowledge gap is further exemplified when the majority of the employees who own a personal computer and use it at work have not invested in good and reputable antivirus software (Raphael et al., 2023).

The subject of ethical conduct is contentious as Kenya ranks high in corruption, especially in the public sector. Employee loyalty in the private sector is not the same as it is in the public sectors and such can be attributed to a lot of factors such as poor remuneration and

working conditions as such employees such government staff are not incentivized to be loyal to their employer (Lukorito, 2012). In such a scenario it becomes easier to tolerate some degree of unethical behavior. For example, a poorly remunerated employee will likely use office resources such as network for personal use such as accessing unsecured websites and social media platforms increasing the risk of unauthorized individuals accessing the organization's network (Lukorito, 2012). In Kenya, it has been observed that some employees use work resources such as laptops for personal use, as such it exposes confidential information to the public. Additionally, personal use of work resources has been established by studies to be an avenue for socially engineered cyber-attacks.

The rate of proliferation of technology in a nation will determine the quality of knowledge an individual possesses in areas such as how to interact with certain types of technology. For example, a nation such as South Korea or the United States of America has a deeper proliferation of technology and the citizens are well versed in information security than Kenyan citizens (Lukorito, 2012). Better knowledge of how technology works is critical to compliance with information security policies. Studies indicate that being aware of the risks of non-compliance will strengthen the overall intent of compliance.

Technology in Kenya is expensive relative to economic status and the purchasing power of consumers. As such majority of computers used in Kenya are refurbished or second-hand. Computers are rather passed down to other users and then taken to a recycling plant (Mikko et al., 2007). Kenya lacks adequate advanced e-waste recycling plants, therefore, organizations that update their hardware choose to donate their old computers to staff or charity. When the storage of outdated systems is not properly erased, there is a possibility of confidential information remaining in the donated hardware (Global, 2023). In

aggregate, several factors affect human behavior which directly affects the compliance ability of people or rather employees to information security. It is more critical than ever for institutions to pay a great deal of attention to the social part of information security as they do to the technology part.

1.1.6 Information Security

As stated by Smith et al. (2006) the general public understands information security as the process of recording, maintaining, and monitoring government agency rules and activities. According to Andrews (1999), information security refers to safeguarding information systems from unauthorized access or modification of data while it is being processed, stored, or transported. It also includes taking the necessary precautions to identify, record, and mitigate any threats to authorized users' access. Privacy refers to the lack of arbitrary and possibly intrusive gathering and use of personal data. As a result, security is a technical factor, but privacy is more social (Langenderfer & Miyazaki, 2009). The goal of information security is to protect the data belonging to an organization as well as the business activities that rely on it (Bell & Greg, 2001). Managing information risks and exposures effectively can directly impact an organization's profitability and overall worth (Oliver et al., 2009).

Reactive approaches are more frequently used in information security. An example of this is the 2011 defacement of the Kenya Police website, which prompted the government's security branch to quickly arrange press conferences in an attempt to salvage its reputation and sway public opinion (Madowo, 2011). According to Scott (2003), the business, legal, and administrative procedures related to the security and preservation of electronic government data are still in the early stages of development. By creating policies and

procedures to increase security, governments are strengthening their preparedness for disasters (Frank, 2003). Breach of information security is highly dynamic in that it is continuously shifting and getting more difficult to identify. According to data acquired from a variety of government organizations, the most significant hurdles when it comes to information security are consciousness, active management assistance training, and enough money (Smith et al., 2006). When information security is employed properly, the cost-benefit analysis justifies the original investment; however, incorrect implementation can have serious implications, including competitive disadvantage and disastrous economic damage (Ataya et al., 2006).

1.1.7 Disposal of Waste Containing Sensitive Information

Waste disposal is the process of getting rid of undesired or pointless objects, materials, or technology. When it comes to information system security, one way that cybercriminals can obtain data that was previously restricted is through waste disposal (Global, 2023). Printed documents, broken optical disks, memory cards, and obsolete technology like computer hard drives are just a few examples of the various types of office waste. Due to increased environmental awareness, most waste is now recycled, and working decommissioned technology is usually donated or resold (Global, 2023). If decommissioned storage media is not properly erased, it may still contain private client data. Similarly, printed paper waste may contain information that recycling participants may access if it is not properly shredded confidential data belonging to the business. In general, information security problems pertaining to waste disposal operations are greatly impacted by human behavior, which suggests a flaw in the information system. Instances where inappropriate waste disposal has resulted in cyberattacks on information systems or allowed unauthorized access to private data are numerous and noteworthy worldwide

(Global, 2023). For example, determining the entire extent of the threat to data on decommissioned media can be difficult. After a device is disconnected from the grid, how can security teams discover a breach? Until the data is discovered for sale on the darknet or an intruder returns and demands a ransom, they are actually unable to do so. If neither of these events occurs, the exploit could continue indefinitely (Global, 2023). It is for malicious purposes, such as selling data on the dark web, creating data profiles using personally identifiable information (PII), or directly breaking into financial or personal accounts, it is possible to access and use data stored on dormant hard drives and devices (Global, 2023). Cybercriminals may demand a ransom in order to unlock data they have stolen from devices that are almost beyond repair. Even in the event that an organization pays the ransom, there is no assurance that the thieves will return the device or data. It is possible that they have already put it up for sale on dark web marketplaces (Global, 2023).

Penalties and legal costs can accumulate rapidly if an IT asset disposal is not done correctly. Recently, Global Bank was willing to pay sixty million dollars in compensation (Global, 2023) to resolve the class action lawsuit concerning legacy equipment that was decommissioned but not properly cleaned. In January 2022, a global bank and financial services conglomerate agreed to pay \$60 million to resolve a class-action claim launched by consumers regarding data breaches that affected practically 15 million current and past customers (Global, 2023). In 2016 and 2019, the international bank retired outdated hardware that held personally identifiable information (PII) belonging to its customers. Following that, computer hardware resellers purchased the equipment (Global, 2023). In 2017, a vendor made contact with the global bank, claiming to have access to client data.

Sensitive data from the legacy equipment was not entirely removed before it was sold. Unencrypted datasets may have been accessed and exposed by unauthorized third parties.

1.2 Statement of the Problem

There are several causes of these security threats. One of them is hiring young employees. Hiring young employees may provide a company with fresh perspectives and expertise, but it also puts information security at risk. Seventy percent of younger workers (generation Z) frequently don't follow established information security guidelines. Given that this generation is accustomed to sharing every aspect of their private lives on social media sites like "Facebook" and "Twitter," how can they be trusted with sensitive business information (Cisco Connected World Technology Report, 2011)? Another aspect is computer literacy. Computer skills are now taught in schools and are required for employment. As a result, employees may use their computer skills to detect flaws and problems in information systems (Gauci, 2008). There is also the issue of ignorance. It is vital to communicate to the system's end users the importance of following security laws. These persons may open emails without scanning them, transmit flash drives and CDs, and share passwords. They will also browse websites with suspicious links, which may endanger government security procedures and expose them to further security risks. End users may be uninformed of security risks and hold preconceived assumptions, attitudes, and beliefs about how information security legislation should be applied (Alfawaz et al., 2008). Information system vulnerability has increased as a result of the government's usage of multiple ICT tools and modern apps (Kessler et al., 2011). These security issues have an influence on government activity at several levels. When information is needed, the government must ensure that data and information processing technologies are available (Evans, 2003).

These risks have the potential to cause denial of service, compromise data integrity, loss of critical information, wasted time recovering data from backups, and significant costs for purchasing firewalls and security software, as well as hiring human labor to handle information security (Alsmadi, 2011). Certain threats also increase fraud and harm the government's credibility (Mbuvi, 2012). Citizens may discourage the government from deploying ICT if they perceive the government's website is vulnerable to attack (Stibbe, 2005).

Similar to robust infrastructures such as SCADA (Smith, 2005) NLIMS' top priority is security, most of the attention has gone into the security towards the technical part of NLIMS. Human psychology or behavior has been shown in several studies to be exploitable. Attackers can exploit human weakness to gain access to NLIMS because it does not require ICT experience to launch a social engineering attack. Socio-technical cyber security approaches have not been extensively integrated in modern cyber security management and this raises the concern that NLIMS is effectively equipped to deter non-technical attacks.

1.3 Objective of the Study

1.3.1 Broad Objective

To assess the effectiveness of NLIMS's non-technical cyber security management approach.

1.3.2 Specific Objectives

- i. To evaluate workstation privacy among employees linked to the NLIMS system.
- ii. To assess office garbage disposal techniques used in workstations and offices linked to the NLIMS system.
- iii. To appraise social engineering awareness by staff linked to NLIMS

1.3.3 Research questions

- i. How do employees linked to NLIMS prevent shoulder surfing from colleagues?
- ii. What garbage disposal techniques are used to prevent dumpster diving?
- iii. Are the staff linked to NLIMS aware of social engineering and ways to protect themselves from being victims?

1.4 Justification of the Study

The findings from this research will benefit the following individuals and entities.

Ministry of land and physical planning

Data from this research will highlight weaknesses and strengths in the non-technical approach to cyber security management. This information will be useful in designing deterrence measures to the weaknesses and a learning point from the strengths by establishing which techniques work best against which attacks or weaknesses.

Government ministries and parastatal

Similar systems such as NLIMS in other ministries can use the data from this research to reinforce their system similar to the Ministry of Land and Physical Planning.

Private firm's corporates and organizations

The same approach that can be adopted by the Ministry of Lands and Physical Planning in response to findings from this research can be adopted by firms running robust information systems

Academic body

Findings from this research will enrich the academic body of knowledge and can be used as stepping stones for further studies.

1.5 Assumptions of the Study

- i. The architectural design of the NLIMS information system is public knowledge or can be accessed with minimal requirements
- ii. Ministry of Land and physical planning staff linked to the NLIMS system can be accessed for interview
- iii. The Ministry of Land and Physical Planning has a functioning non-technical cyber security management approach in play for NLIMS.

1.6 Limitations of the Study

- i. Information about NLIMS information security architecture is accessible by the public or for research
- ii. The staff may not be allowed to respond to some questions
- iii. The ministries may limit the category of staff that can be interviewed which may affect sample pool diversity.

1.7 Scope and Delimitations of the Study

- i. The study focused on Kenya's Ministry of Land and Physical planning
- ii. The study focused on non-technical cybersecurity approaches

1.8 Organization of the Study

The research paper will constitute 5 key chapters. The first chapter will comprise of the following; introduction which is an introductive summary of the entire research. The second is the background of the research from both local regional and global perspectives about the problem the research intends to address. Thirdly is the problem statement and the list of research objectives and research questions, the chapter ends with a justification for the study. Chapter two is the literature review. It will comprise a theoretical framework for

the research and empirical review of published works on relevant topics to the study. It will also include a conceptual framework for the research. Chapter three is the methodology, it includes how the research will be carried out that is research design, data collection tool, data analysis, research limitation, and ethical considerations. Chapter four will constitute data analysis and discussion. Chapter Five will conclude with the research and recommendations.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter consists of, literature and theoretical models that will be contextually appraised in correspondence with the study's objectives. The study will appraise complexity theory in cyber security. This chapter will also evaluate on a theoretical basis how the research variables interact. The independent variable used here human behaviour. The intervening variable is social engineering technics. The dependent variable is non-technical cyber security management.

2.2 Information Security

Information security vulnerabilities in e-commerce and e-government information infrastructure are quite similar (Nikkhahan et al., 2009). The difference comes from the size of the infrastructure. For a simple e-commerce such telecommunication company or an online shopping website, focus on a small group of people and there is less or no codependency between information systems. On the side of the e-government, multiple departments and ministries depend on and rely on data from each other. For example, the Revenue Department depends on data from the Citizen Registration Department and the Huduma Centre relies on data from all government departments. Therefore, a weakness in one system can be a major source of cyber security concern for other departments. Secondly, about information codependency, it is hard for each department to practice information privacy. E-government systems store highly critical and confidential information that pertains to the government as an entity and the citizen, as such information is very important (Conklin & White, 2006). It's further a challenge due to the

codependency (Stibbe, 2005). The type of information that can be illegally accessed in a government e-service is more useful to commit identity theft compared to that which is a product of phishing (Alsmadi, 2011).

About the ever-increasing codependence of the business world and governments on matters of information systems, the agency of information security governance is well appreciated and accepted by leaders. However, the uncertainty that still plagues corporates at all levels is not what or why to secure; that is already catered for by policies and risk management strategies. The uncertainty is on to what extent, how, when and the cost needed to secure information systems remain (Kanhere, 2009). Information security standards and their efficient implementation to safeguard information assets are required due to the growing threats and vulnerabilities in a networked and connected world, the expanding use of information technology in practically all fields, and the high value of information in today's environment. Integrated citizen information is made easier by the effectiveness of electronic data management, but it also brings with it more complicated controls and procedures needs. Common concerns about ubiquitous ICT adoption include ongoing surveillance, misuse of personal data, and invasive data collection.

As stated by Smith et al. (2006) the general public understands information security to be the process of recording, maintaining, and monitoring government agency policies and operations. Andrews (1999) defines information security as protecting information systems from illegal access or alteration of data while it is being processed, stored, or transferred. It also entails taking the required steps to detect, record, and mitigate any threats to authorized users' access. The absence of unreasonable and often intrusive personal information collection and use is referred to as privacy. As a result, security is a

technological concept, but privacy is a social one (Langenderfer & Miyazaki, 2009). Information security aims to protect an organization's information assets as well as the commercial operations they support. The effective management of information risks and exposures may have a direct influence on an organization's profitability and overall value. Reactive techniques are becoming increasingly popular in information security. For example, the 2011 defacement of the Kenya Police website caused the government's security department to swiftly schedule press conferences in an attempt to repair its reputation and impact public opinion (Madowo, 2011).

According to Scott (2003), the commercial, legal, and administrative procedures related to the security and preservation of electronic government data are still in the early stages of development. By creating rules and processes to increase security, governments are strengthening their readiness for disasters (Frank, 2003). Information security breaches are dynamic in the sense that they are ever-changing and getting harder to find. The main challenges in implementing information security are awareness, active management support, training, and adequate budget, according to data gathered from a wide range of government agencies (Smith et al., 2006). When information security is used well, the cost-benefit analysis justifies the initial investment; nevertheless, the consequences of improper implementation can be severe, leading to both competitive disadvantage and catastrophic financial losses (Ataya et al., 2006).

2.3 Information Security Threats

Any situation or event that has the potential to damage an information system by means of illegal access, data loss, disclosure, alteration, and/or denial of service is considered an information security threat (Yang, 2008). Hacking is a prevalent danger that involves

breaking into a computer system to get unauthorized access by evading its security measures (Chandler, 1996). A different danger is a denial of service assault (DOS), in which an attacker overwhelms a server or network with pointless orders, exhausting its resources and rendering the service unavailable (Alfawaz et al., 2008).

There's also the threat of spam. Sending unwanted mass communications to a large number of people at once—possibly up to thousands—with the primary goal of promoting items to prospective clients is known as spamming (Chandler, 1996). A further hazard is malware assault. Malware spreads by using well-known means of communication, such as Trojan horses downloaded from websites, worms sent through email and messages, and virus-infected files downloaded from peer-to-peer connections. It can also originate from removable media, such as thumb drives, compact disks, and mobile devices that are connected to computers (Yang, 2008).

Threats might also come from software defects. A computer program or system fault is defined as an error, defect, mistake, failure, or fault that results in an inaccurate or unanticipated outcome or leads it to act in an undesired manner (Yang, 2008). Users with excessive privileges might potentially pose a hazard. Just enough authorization should be granted to users to carry out their responsibilities (Chandler, 1996).

There are many factors that cause these security threats. One of them is hiring young employees. Hiring young employees can bring fresh talent and innovation to an organization, however, they are also a source of information security risk. 70 percent of Generation Y (younger employees) frequently ignore laid-down information security policies. If this age group is accustomed to sharing complete details about their personal lives on social media sites like “Facebook” and “Twitter”, how can they be entrusted with

company-sensitive data (Cisco Connected World Technology Report, 2011)? Computer literacy is also another factor. Computer studies are part of today's school curriculum and a key requirement to finding employment.

These security risks are caused by several reasons. One of them is employing youthful workers. Although hiring young workers may infuse a business with new ideas and skills, it also poses a danger to information security. Seventy percent of younger employees, or members of Generation Y, often disregard established information security regulations. How can this age group be trusted with critical corporate information if they are used to disclosing every detail of their personal life on social media platforms like "Facebook" and "Twitter" (Cisco Connected World Technology Report, 2011)? Another element is computer literacy. These days, computer studies are taught in schools and are essential to getting a job (Chandler, 1996). As a result, workers may utilize their computer expertise to identify weaknesses and issues in information systems (Gauci, 2008). One more aspect is ignorance. It is necessary to explain to the system's end users the significance of adhering to security regulations. It is probable that these individuals may open emails without scanning them, transfer flash drives and compact disks, and exchange passwords. They will also visit websites with dubious linkages, so these activities might jeopardize government security measures and put them at risk for other security issues. It's possible that end users are unaware of security issues and that they have preconceived notions, attitudes, and beliefs about the application of information security regulations (Alfawaz et al., 2008). Information system insecurity has risen as a result of the government's use of numerous ICT tools and contemporary applications (Kessler et al., 2011). Government activities are impacted by these security risks on a number of levels. When information is needed, the

government must make sure that data and information processing systems are accessible (Evans, 2003). These risks have the potential to cause denial of service, compromise data integrity, loss of important information, wasted time recovering information from backups, and significant expenses for purchasing firewalls and security software as well as hiring human labor to handle information security (Alsmadi, 2011). Certain dangers also result in a rise in fraud and damage to the government's reputation (Mbuvi, 2012). Citizens may dissuade the government from implementing ICT if they believe that the government website is vulnerable to assaults (Stibbe, 2005).

2.4 Theoretical Framework

The Complexity Theory

Mason (2022) the central thesis of complexity theory posits that in every behavior of complex systems, there is an underlying order to which a complex system is a system in whose parts and their interaction together embody a unique behaviour, which cannot be properly exemplified by the mere analysis of all its constituting components (Gandhi, 2014). Gandhi adds that the relationship is non-linear and the cause and effect cannot be necessarily linked. Gandhi based on Morin (1992) posits that for a system to be complex it has to satisfy the following characteristics;

- I. It is not possible to anticipate the behavior or outcome by only examining the system's components and inputs, as mentioned in Gandhi (2014).
- II. The system's behavior is emergent and varies over time. As stated in Gandhi (2014), the same input and environmental circumstances do not necessarily ensure the same outcome.

- III. A system's players, or its agents—in this case, human agents—are self-learning and adapt their behavior in response to the lessons learned from earlier experiences, as stated in Gandhi (2014).

Holism approach to cyber security

This research posits that cybersecurity management should be approached holistically. Gandhi propounds that despite complex barriers set up to deter cyber-attacks most often attackers still manage to break through (Gandhi, 2014). Gandhi, states that. “More often than not, computer break-ins are a collision of circumstances rather than a standalone vulnerability being exploited for a cyber-attack to succeed. In other words, it’s the “whole” of the circumstances and actions of the attackers that cause the damage” (Gandhi, 2014) Most cyber security management approaches are based on a reductionist ideology (McLeod, 2008) this is basically focused constituent parts of the system and the causality, as opined by Gandhi it has a robust practical use case. Under the lens of reductionist cyber security is approached from a specific point solution where attacks on known vulnerability can be anticipated (Gandhi, 2014). In the modern cyber system, there are systems such as human behavior and socio –cyber systems to mention a few that a reductionist approach is limited. A holistic approach to cyber security is analogous to the immunity of biological beings that are robust, adaptive, and constantly learning the ever-dynamic behavior of threats such as the mutation of a pathogen. With that in mind technical vulnerabilities which are human-based and influence cannot be effectively managed in the same way as technical vulnerabilities.

Drawback

The main challenge to this theory is that there is limited practical application that can be sufficiently used to benchmark. This is due to its early adoption.

Complexity-based approach to Mitigating security threats

Non-technical vulnerability and threats change, evolve, and adapt based on the environment they are in, and thus form a complex cyber security system cause and effect cannot be linearly predicted (Armstrong et al., 2009). It has been shown that a systematic reductionist approach may not be effective in such regard (McLeod, 2008). The central thesis for this study is to evaluate indirectly if the Ministry of Lands in Kenya has an effective approach to deter non-technical threats on non-technical vulnerabilities. Complex-based approaches to cyber security have limited practical evidence but a promising use (Gandhi, 2014). This theoretical model is used to exemplify the true nature of non-technical threats and non-technical vulnerability and how conventional reductionist approaches have limited usability. This study uses this model to show how limited they can be.

Drawback

This theory propounds the use of complex approaches such as Agent-Based Modelling (ABM) to non-technical aspects of cyber security and also when both technical and non-technical are approached as one holistic complex system. However, ABM is a complex approach outside the scope of this research, a more practical approach is the social-technical system (STS) (Konstantinia & Andrew, 2013).

Social-Technical System

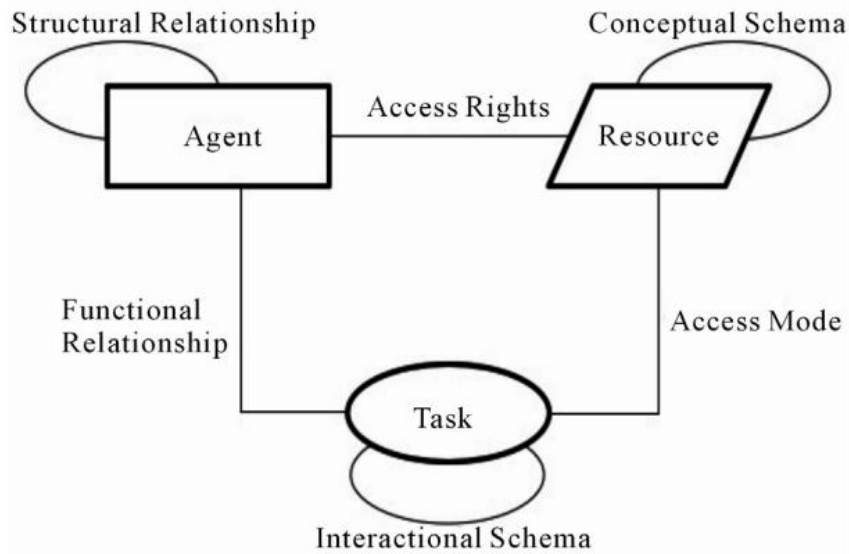
Socio-technical system approach considers the hardware, software, personal, and community components of a system designed for a particular purpose (Norman, 2022). It is therefore a mixture of people and technology (Rangwala, 2022). STS provides an opportunity to isolate ethical errors and risks in the social aspects of the systems. It consists of many items. It consists of five critical components, people, hardware, software, data, and Law and regulations (Rangwala, 2022).

The ART Model of Socio-Technical Systems

This model was proposed and designed by Konstantin Charitoudi and Andrew Blyth. The primary objective of the model is achieved by the use of reasoning to connect both the ICT infrastructure and the business processes, as a socio-technical approach (Konstantinia & Andrew, 2013). This model offers an ontological and taxonomic overview of the whole system therefore offering an opportunity to view the system components and how they interact with possible points of weakness (Konstantinia & Andrew, 2013).

Figure 2.1

A socio-technical cybernetic enterprise model



The figure above shows the taxonomical and ontological view of the system from the socio-technical perspective. We can isolate people as agents, access rights as rules and regulation software, and access mode from the technical system. The area of interest is the functional relationship and interactional schema, these two components comprise the roles of the agents, inter-agent interaction and relationships, their obligations, and the formal tasks as described by their roles. This forms the social aspect of a system and is entirely human-based meaning it is predicated by human shortcomings and errors.

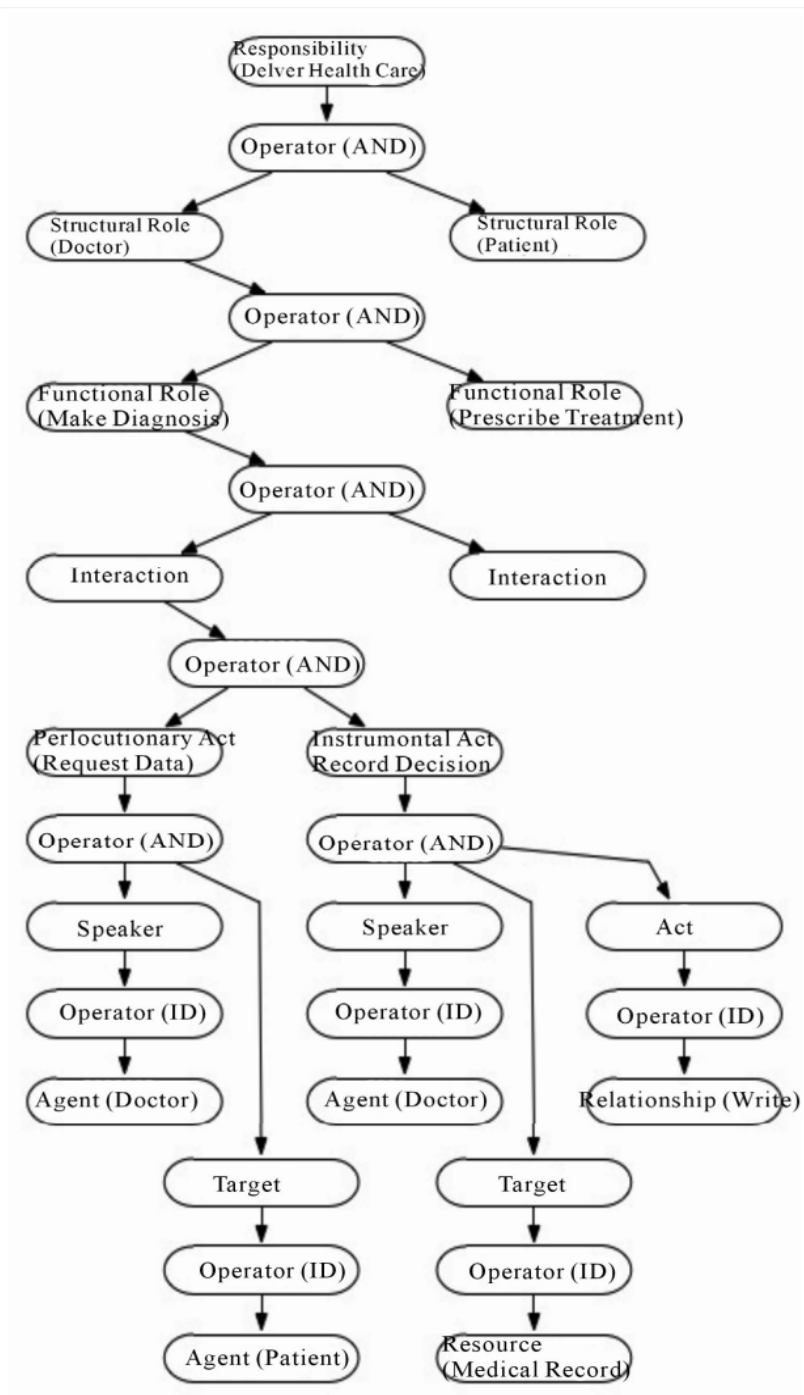
In the process of cyber security risk management, it is critical to properly understand the relationship and the interaction between the people and the technical component. Each person in an organization has a responsibility. Their responsibility is linked to the tasks they execute within the organization. Therefore, key changes or manipulation of the system is achieved through tasks. In this case, the function of the role a person plays in an

organization is to define their behavior about the interaction that a person partakes while executing their task. The function here offers an opportunity to illustrate all necessary conditions that must be adhered to before the responsibility is achieved (Konstantinia & Andrew, 2013). These conditions are requirements for certain roles to be performed by particular agents who are employees. Thus according to Konstantinia and Andrew's, an obligation is a function that takes a responsibility as input and maps that responsibility to the set of roles that must be performed in order for the responsibility to be fulfilled. A classic example is that of an educator whereby a teacher who is an agent has the responsibility to educate the students. The responsibility consists of the obligation that the teacher must partake in a set of roles such as grading assignments or setting examinations. The set of roles can depend on each other and also the teacher as an agent can interact with other teachers and influence their roles creating a responsibility dependency. Responsibility dependency can be further illustrated in a learning organization where to educate students, several teachers must deliver lectures agree on a set of questions to test, externalize the test administer the test to the large student pool. The teachers again have to collaborate to grade the test. This indicates that for a student to come out of an institution as satisfactorily educated, the individual responsibility of a teacher depends on their colleagues. Using a healthcare organization, as a model example the flow chart can be constructed to illustrate a responsibility dependency tree (Konstantinia & Andrew, 2013).

This model will be used in this research as a reference model that will help in constructing an exploded view of NLIMS for the purpose of isolating possible weaknesses or strengths.

Figure 2.2

Responsibility dependency



2.5 Empirical Literature Review

2.5.1 Human cyber security errors

This section outlines the many cyber security faults made by frequent computer users. According to several reports such as Furnell and Clarke (2012) and Schneier (2004) humans are the most vulnerable to security threats, which is reinforced by more recent findings. According to one statistic, human error accounts for 95% of cyber and network threats (Noble, 2018). People in these situations are characterized as security professionals or computer system users (King et al., 2018; Andrade and Yoo, 2019) while the majority of research in this field focuses on errors made by computer system operators. According to Ifinedo (2014), the most susceptible component in system security is the company's workers. Human errors that can affect network and cyber security include password sharing and oversharing content through social media, visiting fraudulent websites, using unapproved outside media, clicking at random links, constantly entering the same passwords, opening email attachments from suspicious sources, sending private data over mobile networks, failing to physically secure individual electronic devices, and failing to update software. As a result, enhancing the accessibility and usability of a network or data while maintaining security is a fundamental issue that underlies information and cyber security (Veksler et al., 2018). Organizations routinely seek complex passwords from computer users in order to increase security, which may be incredibly difficult to use. People who use computers regularly, on the other hand, choose the simplest solution, such as using a weak password and the same password for many websites.

The previous study on the three categories of human security blunders (installing software updates, sharing usernames and passwords with others, and falling for phishing) is discussed below. Getting taken in by phishing. Some phishing research employed a laboratory-based phishing experiment (Jakobsson & Ratkiewicz, 2006; Jagatic et al., 2007).

Recent research has demonstrated the importance of laboratory-based phishing testing in practical spoofing (Hakim et al., 2020). According to one research, more than 30% of government employees clicked on a questionable link in this phishing email, and many of them shared their passwords (Baillon et al., 2019). A similar phishing experiment was used in another study, and around 60% of university students clicked on a suspicious link in an email spoofing (Diaz et al., 2018). As a result, some studies by Hamill and Deckro (2005) and Jones and Colwill (2008) argue that human aspects, behavioral studies, and psychological research must be considered in network and cyber security investigations. It took people approximately four rounds before they discovered they were receiving phishing emails, in accordance with a different research study conducted by Bowen et al. (2014) on how students and faculty at Columbia University respond to phishing emails. In line with Curtis et al. (2018) a recent study additionally found an association between computer users' Dark Triad characteristics Machiavellianism, narcissism, and psychopathy—and the success of phishing attacks. This study observed a correlation between a higher propensity to fall victim to phishing attempts and high narcissistic scores along these lines.

As a result, it has been shown that sensitivity to phishing attempts is associated with neuroticism (Halevi et al., 2013). Gonzalez and colleagues discovered in a different study

(Rajivan and Gonzalez, 2018) that effective phishing was more closely associated with the employment of certain hacking methods, such as sending out excessive quantities of notifications and professing shared interests. According to one study, people's reactions to phishing emails remain unchanged despite being warned about them (Mohebzada et al., 2012).

The Human Elements of Security of Information Questionnaire (HAIS-Q) was used to assess participant behavior in a laboratory-based phishing experiment. The findings revealed that individuals with high HAIS-Q scores outperformed other participants (from a corporation, (college, school, etc.) who accidentally received a phishing email asking them to provide their password. According to Herath and Rao's 2009 research, computer users often underestimate their probability of being victims of security breaches and cybercrimes. Exchange of passwords: Sharing passwords with friends, relatives, or even total strangers is a typical human cyber security blunder. Whitty et al. (2015) discovered that password sharing is more widespread among older persons who excel at persistence and self-monitoring. Sharing passwords can lead to one of the most common forms of abuse: financial exploitation of older adults (Bailey et al., 2015). This is especially true for strangers and the internet since many older folks have a high level of trust concerns. Similar to elderly individuals, but younger. Whitty et al. (2015) discovered that password sharing is more widespread among older persons who excel at persistence and self-monitoring. Sharing passwords can lead to one of the most common forms of abuse: financial exploitation of older adults (Bailey et al., 2015). This is especially true for strangers and the internet since many older folks have a high level of trust concerns. Younger folks, like older adults, exchange passwords, particularly for streaming services. According to Smith

(2003), younger users who had grown up with computers perceived security as a hurdle that they needed to overcome. Password sharing is usually 2.4.2. Individual differences that underpin cyber security initiatives.

Individual variations in personality, cognitive, and behavioral qualities have been linked to cybersecurity behavior. According to Thomson and Dawson (2018), individual differences in cognitive abilities and personality traits can have a substantial influence on the success of computer and information system security. We'll go over a couple of these psychological traits below.

Delayed action: Adopting security principles may be associated with mental processes such as using significant effort to achieve a goal. One measure, known as the "need for cognition" scale (Lin et al., 2016), assesses how hard one works, how much one likes, and how often one engages in thinking-intensive activities. As a result, Egelman and Peer (2015) revealed a link between the Need for Cognition (NFC), or the desire to participate in cognitive activities, and performance on the Security Behavior Intentions Scale (Cacioppo et al., 1984). It's noteworthy that a recent study developed a scale to measure procrastination in children and teens, making it relevant to the expanding population of young internet users (Keller et al., 2019). According to McBride et al. (2012) and Shropshire et al. (2006), discovered a link between conscientiousness, or the willingness to adhere to information security procedures and thoroughness. Furthermore, Egelman and Peer (2015) observed a correlation between procrastination and performance on the Security Behaviour Intentions Scale, with procrastinators being less inclined to follow security regulations. This conclusion was reached utilizing the General Decision-Making Style (GDMS) scale (Scott & Bruce, 1995). This makes sense given the negative link

between procrastination and activity participation (Sarmany-Schuller, 1999). Individual differences in impulsive conduct may also be associated with adherence to security standards. Barratt Impulsiveness Scale scores, according to Egelman and Peer (2015), are connected to Security Behavior Intentions Scale performance.

Another study revealed that impulsivity and internet addiction are indications of risky behavior (Hadlington, 2017). As a result, Hu et al. (2015) established a relationship between information security policy breaches and individual differences in self and cognitive control, which is an important component of impulsive actions. Wiederhold (2014) revealed that those who want rapid pleasure are equally vulnerable to cybersecurity threats. Thinking about the long-term consequences of one's actions is an important aspect of impulsivity (for example, saving money now to purchase a house later vs. spending all money now to enjoy life). Thinking ahead: Crucially, following to security principles may be connected with forward-thinking and how present activities would affect future consequences (Moustafa et al., 2018a; Moustafa et al., 2018b). To put it another way, forward-thinking individuals may adhere to security principles to secure the long-term safety of their computer system. In line with this, Egelman and Peer (2015) found a link between Consideration for Future Consequences (CFC) and performance on the Security Behavior Intentions Scale (Joireman et al., 2012). Items on this scale such as "I think it's important to take warnings about negative outcomes seriously even if they're not immediate" and "I consider how things might be in the future and try to influence those things with my day-to-day behavior" are extremely relevant to cyber security behavior. When the unpleasant outcome will not occur for a long time, and "when I make a decision, I consider how it might affect me in the future."

Risk-taking behavior is another psychological trait associated with cyber security. According to some studies, those who use computers often and take risks may be more likely to become victims of cybercrime (Henshel et al., 2015; King et al., 2018). According to Saleme et al. (2018), taking a risk is defined as behaving in a way that has an unclear outcome, usually to obtain more. For example, stealing a bank involves the danger of discovery. It is harmful to ignore security policies since there is no added advantage to doing so, such as pleasing software upgrades, but there is a risk of being a victim of phishing or cybercrime. Another example is knowing of a data breach in which your login and password, among other personal information, were compromised but nothing to change your password. To protect their networks or computer systems, users must select whether to put in more effort (which is safer but involves more labor) or less effort (which results in less safety). Egelman and Peer (2015) found a link between the Security Behavior Intentions Scale and the Domain-Specific Risk-Taking Scale, which includes questions on typical risk-taking behaviors in everyday life (Blais & Weber, 2006; Saleme et al., 2018; Saleme & Moustafa, 2020).

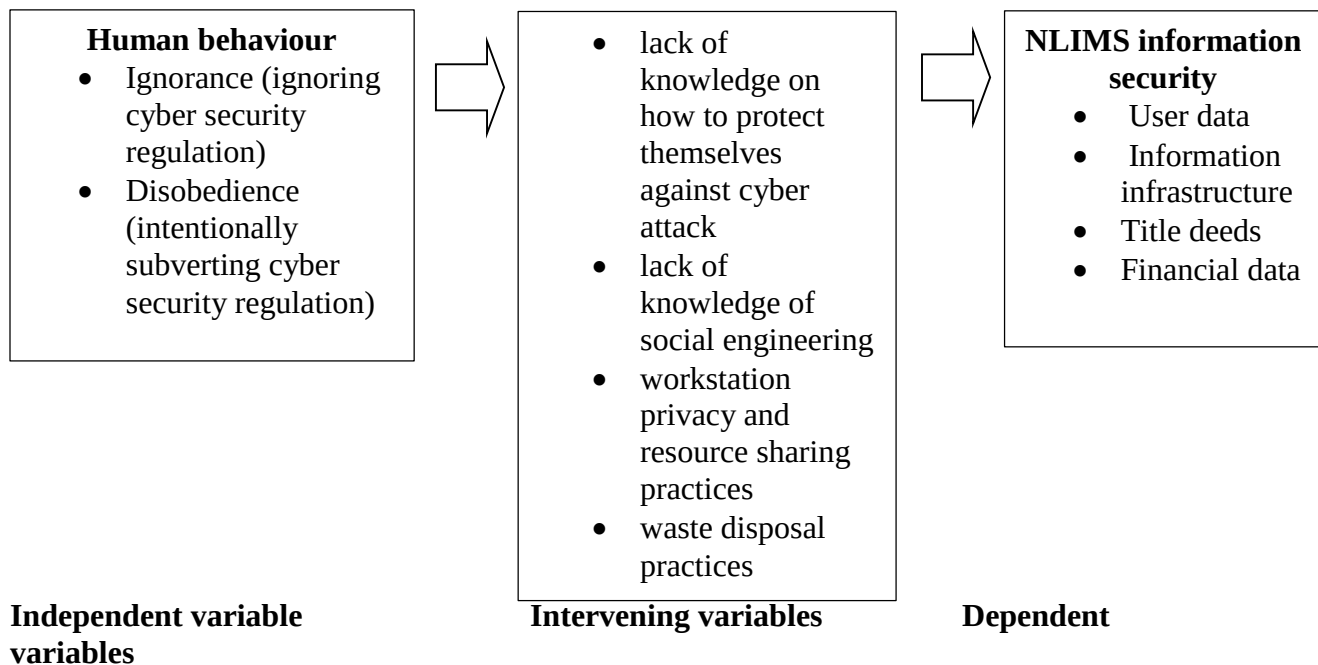
Hadlington et al. (2017) and Hadlington and Murphy (2018) found that using the Risky Cybersecurity Behaviors Scale, Security Behaviours Intentions Scale (SeBIS), and Attitudes toward cybersecurity and cybercrime in business (ATC-IB) in multiple studies, heavy media multitasking is linked to risky cybersecurity behaviors and increased cognitive errors. Optimism bias is linked to making choices based on risk. Psychology has not looked at human optimism bias in great detail (West, 2008; Sharot, 2011; Moutsiana et al., 2013; Garrett & Sharot, 2017). People frequently believe that everything will work out for the best and that they are safe (West, 2008). Put differently, individuals tend to be more

positive and encounter fewer bad events. For example, the majority of individuals underestimate their risk of developing cancer and don't believe it will happen to them. This is pertinent to studying the psychology of cyber and network security as computer users may tend to minimize the importance of cyberattacks or crimes happening to them. For example, research discovered that people are more susceptible to cybersecurity threats when they have an optimism bias (Wiederhold, 2014).

2.6 Conceptual Framework

Figure 2. 3

Diagram indicating the interaction of variables



2.7 Research Gaps

About the empirical review above, a lot of studies have been done in the technological area of cyber security. There is a theoretical approach to the social aspect of cyber security that lacks enough real-life practical utility. Less data has been collected to fully express the

severity of the weaknesses that are associated with the social aspect of information systems. This study intends to contribute data in this area. This data provided proof and necessitated a change in measures to reduce the weakness.

2.8 Summary of the Chapter

The complexity theory suggests that complex systems have unique behaviors that cannot be predicted by analyzing their components. A holistic approach to cyber security, focusing on the whole system rather than just the components, is more effective in managing non-technical vulnerabilities. This approach is analogous to the immunity of biological beings, which are adaptive and constantly learning. However, it has limited practical application due to early adoptions. The complexity-based approach to addressing non-technical threats, such as Agent-Based Modelling (ABM), is more practical and has limited practical evidence.

The socio-technical system approach (STS) focuses on the hardware, software, personal, and community components of a system designed for a specific purpose. It isolates ethical errors and risks in the social aspects of the systems. The ART Model of STS connects ICT infrastructure and business processes, offering an ontological and taxonomic overview of the system. It emphasizes the functional relationship and interactional schema, which form the social aspect of a system. In cyber security risk management, understanding the relationship between people and technical components is crucial.

Humans are considered the highest security vulnerability, with 95% of cyber security incidences being due to human errors. Common human security mistakes include password sharing, oversharing content, utilizing unauthorized material, clicking on random links, inputting the same passwords, reading email attachments from dubious sources,

transmitting confidential information over mobile networks, not physically locking down individual electronic devices, and not updating software are all examples of fraudulent website visits. Organizations frequently ask users to choose complex passwords, yet a lot of people use simple passwords or use the same password across several websites. Research has demonstrated a connection between behavioral and psychological studies, human variables, and susceptibility to phishing attempts. Younger people exchange passwords, especially for streaming services, while older adults—who score higher on persistence and self-monitoring—share passwords more frequently. The effectiveness of protecting computer and information systems can be strongly impacted by individual variances in personality, cognitive ability, and behavioral characteristics.

Egelman and Peer (2015) identify a relationship between the Need for Cognition (NFC) and performance on the Security Behaviour Intentions Scale. Procrastination and internet addiction are indicators of dangerous cyber behavior, with impulsivity and internet addiction being key factors. Adherence to security guidelines is also linked to thinking ahead and considering the future. Risk-taking behavior, such as taking risks with uncertain results, is also linked to cybersecurity. Prolonged multitasking on media is linked to unsafe cybersecurity practices and a rise in cognitive mistakes. This is related to optimism bias, where people tend to underestimate the significance of cyberattacks or crimes, making them more vulnerable to cyberattacks. Understanding these psychological factors can help improve cybersecurity practices and reduce cybercrime risks.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

The methodology of this research is covered in this chapter. It consists of a description of the research location as well as the units used for measurement and goal analysis. It also includes the research design, which serves as the framework for the organization of this investigation. The study population and the selection criteria are discussed. Techniques for gathering and analyzing data are also demonstrated. The ethical concerns are finally mentioned.

3.2 Location of the Study

The site is Nairobi County at the Ministry of Land and physical planning headquarters. The ministry has offices in all counties in Kenya but the study considered Nairobi because NLIMS was first rolled out here and its integration is better than in the rest of the counties. The study seeks to assess human behavior as the independent variable and how it affects the non-technical cyber security management approach amidst intervening variables of the ever-evolving social engineering methods.

3.3 Research Design

The study utilizes a descriptive research methodology since it focuses on measurable numbers and prepares qualitative claims about people or events (Kothari, 2004). Descriptive research design is chosen for this research because it enables actual reporting of the state of affairs with regard to the interaction of both independent and dependent variables. The design enables the study of multiple variables at the same time (Erik & Marko, 2011). Considering that to understand the interplay between independent and dependent variable intervening variables are key because they influence the relationship of

the study. Secondly, the design enables a larger amount of data to be gathered at a relatively low price (Saunders et al., 2012). About data, this study uses both qualitative and quantitative where the two data types adopted to work synergistically to exemplify the relationship under study. The type of descriptive design is descriptive survey design. Survey study/ research is one of the most necessary areas of measurement in modern-day business research. It entails asking the respondent questions to gain insight critical in answering the research question. In aggregate, the survey of this paper was a detailed interview with respondents.

Based on the study objective both qualitative and quantitative data are needed to describe the nature of interaction between the variables the qualitative data are presented as qualitative statements with corresponding gaged answers. These statements were used to gauge the level of cyber security awareness which cannot be easily quantified using quantitative technics.

The study focused on the description of the nature of the impact of the independent variable for inferential purposes. The data was collected through the administration of questionnaires to respondents. The researcher administered the questionnaire in person to increase the interaction with respondents. The research design is adopted based on its adequacy to fulfill the research objectives.

3.4 Target Population and Sample Selection Procedures

A study population is a collection of people or items that are the focus of scientific research (Mugenda & Mugenda, 2012). For this study, the target population – individuals from which the desired information is obtained- is the Staff of NLIMS (Kothari, 2014). The sample population was limited to 300 individuals. There is no necessity for a sampling

frame because respondents are comprised of a specific unique group found in one specific location, which is staff linked to NLIMS.

Sample size can be defined as a subset of the population representing the entire population (Prashant & Supriya , 2010). The right sample size should accomplish the necessity for efficiency as well as representativeness. Magigi proposes Slovin's formula by Taro Yamane (1967) cited in Jeffry and Joyce (2012) or calculation of sample size (Stephan et al., 2015).

$$n \approx \frac{N}{(1+N(\varepsilon)^2)}$$

Where n = Sample size (Staff linked to the NLIMS to be interviewed)

N = Population (Total number of staff linked to the NLIMS)

e = Level of precision (5 – 10%)

our N sample population is 53 individuals therefore, based on the above formula the sample frame n sample frame is 40

Slovin's formula source: (Jeffry & Joyce, 2012)

Non - Non-probability sampling was used to isolate the key population by use of the quota sampling technique. Singh and Masuku (2014) suggest this method if the research has a preset determinant that the key population must meet. The determining key factor is the staff working in the Ministry of Land and Physical Planning must; have access to the NLIMS system via a workstation or subordinate to one.

3.5 Data Collection Instruments

Face-to-face interviews were used to gather data, along with the delivery of questionnaires. The questionnaire contained close-ended questions and statements with a range of multiple

choices to collect qualitative and simplify encoding them. In research, a data collection instrument is a device that specifies and objectifies the data collection process. Instruments are typically written and may be given directly to the subject to collect data or may provide an objective description of the collection of specific types of data (Macnee & McCabe, 2006 as cited in Kettler, 2019). Questionnaires, interviews, timetables, and existing data are all possible data-gathering devices. Questionnaires served as the primary data-gathering tool in this investigation.

Unstructured questions were used in the study to provide respondents the freedom to react with their own responses. These questions are easier to design, allow for a more in-depth answer, and provide insight into the respondent's past, sentiments, underlying reasons, interests, and decisions. Structured closed-ended questionnaires were employed in the study to collect data. Before beginning the data-collecting process, the researcher sent a cover letter together with the questionnaire to each study participant, outlining their expected role and stressing the need to provide truthful information. The participants were also given the assurance by the researcher that their information would be handled with absolute confidentiality. In order to protect anonymity and prevent potential victimization from any source, the responder was given an envelope labeled "questionnaire" along with their thesis subject. Once the questionnaire was completed, they were instructed to seal it. The investigator has made certain that participants have sufficient time to finish the surveys. The questions were closed-ended and included subheadings to help the responders when needed.

3.6 Data Processing and Analysis Procedures

While inferential statistics are frequently employed in presenting results, descriptive statistics are the most basic method of summarizing data and are necessary for understanding the outcomes of quantitative research (McMillan & Schumacher, 2001). Similar to this, Creswell (2005) explains that inferential statistical tests are used to evaluate the differences, relationships, and correlations among variables in the data set, whereas descriptive statistics summarize a single variable in a data set or compare how one score relates to all others. Descriptive statistics including the mode, mean, and standard deviations were used to assess the raw data. To examine the link between the independent and dependent variables, inferential statistics, correlation index, and linear regression were employed.

3.7 Piloting of Research Instruments

The instruments have to be pre-tested on a sample of ten or more respondents, who don't have to be typical of the population mentioned by Crispiness (2012) and according to Babbie (2003). Only one pilot study was conducted where ten research colleagues in the department were randomly chosen as respondents, and they were given a questionnaire. The data gathered was utilized to assess the reliability of the surveys using the MANOVA and Pearson coefficient index.

3.8 Validity of Research Instruments

This study does not use large data sets therefore, the Principal Component Analysis (PCA) test was not adopted. PCA is more useful in large-data (Abdi, 2010). For this case, the MANOVA test was loaded in Excel XLSTAT to conduct the one-way MANOVA, where y represents the dependent variable and x represents the independent variable. For this test,

a null hypothesis was adopted which indicates no significant relationship between the variables. For the test result, we focused on the Wilks Lambda test where the lower lambda value in correlation to the independent variable, indicates a significant effect that the independent variable has on the dependent variable (Keselman, 2016). Our lambda value in the test is 0.036 which is lower than the recommended significant value of 0.05. Therefore, the adopted null hypothesis is rejected projecting that the selected variables have a significant impact on each other.

3.9 Reliability of Research Instruments

The data collected during the pilot stage were collected in such a way as to collect two data sets in two weeks the data set was used to carry out a test-retest by use of the Pearson coefficient index. This was to gauge the reliability of the data collection instrument. This test was opted despite some weaknesses the intention to see if the instrument could meet a minimum reliability test (Chrispinus, 2012). The correlation coefficient between the two data set was 0.743 which is closer to 1 indicating a positively strong correlation (Chrispinus, 2012).

3.10 Summary of Research Objectives, Hypotheses, and Analytical Models-100

The study objectives are first, to evaluate workstation privacy among employees linked to the NLIMS system to establish the status of shoulder surfing. The second objective is to assess office garbage disposal techniques used in workstations and offices linked to the NLIMS system, this is to establish how secure is process in which waste that contains confidential is disposed of. The third objective is to appraise the awareness of social engineering by staff linked to NLIMS, this objective aims to gauge information security awareness of the staff linked to NLIMS. The following questions were answered by the

study; How do employees linked to NLIMS prevent shoulder surfing from colleagues? What garbage disposal techniques are used to prevent dumpster diving? Are the staff linked to NLIMS aware of social engineering and ways to protect themselves from being victims?

3.11 Operationalization of Study Variables

The first objectives were tested through the data collection and conductive preliminary descriptive statistical analysis. For the first objective, the data was collected on the following key areas, the presence of shoulder surfing by staff of different ranks, those that are linked to NLIMS, and those that are not. This data was gauged in terms of the frequency of shoulder surfing by colleagues. Data was also being collected on shoulder surfing incidences outside work, especially at home. Data was also collected on the type of work resource sharing, the type of resource, and the frequency at which each resource is shared. Such resources include a workstation desk, storage media such as thumb drives, external hard drives, printer, and file storage cabinet. This helped reveal ways in which confidential information can be accessed by unauthorized personnel through innocent resource sharing. The second objective is about waste disposal, data was collected in key areas which were different materials such as printed papers, and storage media disposed of, the study also looked at the type of disposal approaches, from here we gauged which approach was secure and the frequency of use of each approach. The approaches for waste disposal under study were physical damage to storage media, burning, use of waste bin, shredding, use of recycling companies, and repurposing of decommissioned storage devices for personal use by staff linked to NLIMS. The third variable is social engineering awareness, data was collected in the following areas general awareness on how to protect oneself against cyber-

attacks, how to detect an attack, knowledge and importance of an antivirus, and the agency to be cautious of cyber-attacks.

3.12 Ethical Considerations

The researcher asked Kenya's National Council for Science and Technology for authorization to carry out the study. This is to guarantee that research is conducted in accordance with national legislation. It is critical that all participants in the study maintain the highest level of secrecy and display unwavering honesty. Additionally, the research made sure that nobody gets hurt or has negative outcomes. Thus, in order to guarantee that no responder experiences bodily injury, discomfort, suffering, shame, or any other type of loss, the researcher would conduct the following actions.

- The researcher also respected the autonomy principle by making sure that the participants were fully informed about the purpose, risks, rewards, and available options of the study.
- The researcher also adhered to beneficence, meaning that over the course of the study, he considered how to maximize benefits and minimize potential damage.

The proper protocol was observed while seeking an audience with members of the national government, and the interviews were carried out according to the ministry's instructions. Every internet source was referenced along with its corresponding copyright marking. The respondent's confidentiality was maintained by their policies (their right to privacy was respected). When restrictions are necessary, important attention to confidential government information is maintained.

3.13 Summary of the Chapter

In aggregate, the study also adopted a descriptive research design and analytical models to answer research questions. The study site is NLIMS headquarters where 40 respondents were interviewed. Primary data was collected using a questionnaire and secondary data was collected through examination of past financial and relevant reports. A pilot study was used to test the reliability of data collection instruments and the validity of the data was tested in conformity with the study variables. Data was descriptively and inferentially analyzed with selected statistical tools mentioned earlier.

CHAPTER FOUR

RESULTS AND DISCUSSION

4.1 Introduction

This chapter includes an examination of the data collected using the research instruments outlined in Chapter 3. Section 4.2 provides information on the questionnaire response rate. Section 4.3 presents an overview of the findings in tabular and graphical style. Section 4.4 presents descriptive and inferential statistical analyses of the data. Section 4.5 presents a contextual overview of the statistical study.

4.2 The Study's Response Rate

Data for this study were collected via questionnaires. The sample size for this study was 40 respondents (20 males and 20 females). Of the 40 questionnaires distributed, 40 were completed and returned to the researcher, giving a 100% response rate.

4.3 Summary of the Study Results

The study's goals led the researcher to evaluate critical issues, including how NLIMS workers dispose of garbage containing information or data from their day-to-day operations. Second, the level of workstation privacy, and third, the staff's awareness of social engineering threats. The summary of the data acquired in accordance with the research goals is as follows:

4.3.1 Access Control (test factors: waste disposal, should surfing) **Printed document Waste Disposal (Sample size = 40)**

Table 4.1*Printed document waste disposal*

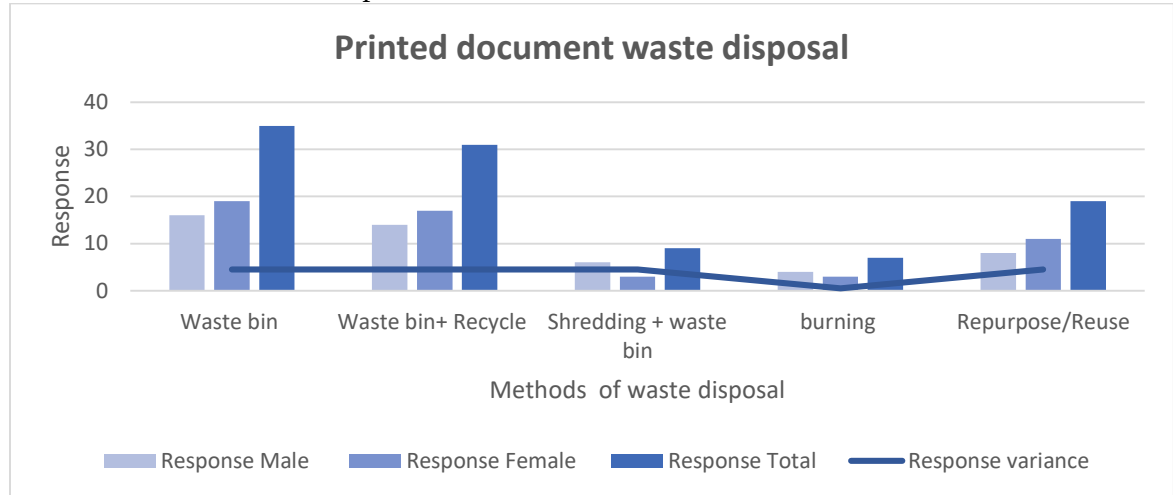
<i>Ways to dispose</i>	Response			
	Male	Female	Total	Variance
<i>Waste bin</i>	16	19	35	4.5
<i>Waste bin+ Recycle</i>	14	17	31	4.5
<i>Shredding + waste bin</i>	6	3	9	4.5
<i>burning</i>	4	3	7	0.5
<i>Repurpose/Reuse</i>	8	11	19	4.5

NB: each waste disposal method is an independent survey; this was conducted to test the level of preference for each method because multiple methods can be used by one individual depending on their preference.

From table 4.1, it is clear that waste bin at 77.5% and waste bin + recycle at 87.5% are the two desirable methods that the staff linked to NLIMS prefer to use to dispose of printed paper waste. This high percentage indicates that the majority of waste printed paper can be accessed by the public as waste. These two methods do not safeguard the NLIMS system against dumb star diving- an avenue for cybercriminals to access data that is instrumental in launching attacks against NLIMS. Only 15 % prefer shredding paper waste before waste disposal and 10% prefer burning which is the 100% effective way of disposing of printed paper waste which may contain usable data for the cybercriminals.

Figure 4.1

Printed document waste disposal



Shredding before disposal makes it hard to reconstruct information from printed paper waste. In aggregate, 25 % (burning 10%, and shredding 5%) constitute effective methods of properly securing printed paper waste disposal while 75% unsecured methods. Finally, the need to securely dispose of waste is apparent for male staff more than it is for female staff where male staff prefers shredding at 67% while females at 33% and 57% of male staff prefer burning to 42 % of female staff.

4.3.2 Storage Media Waste Disposal

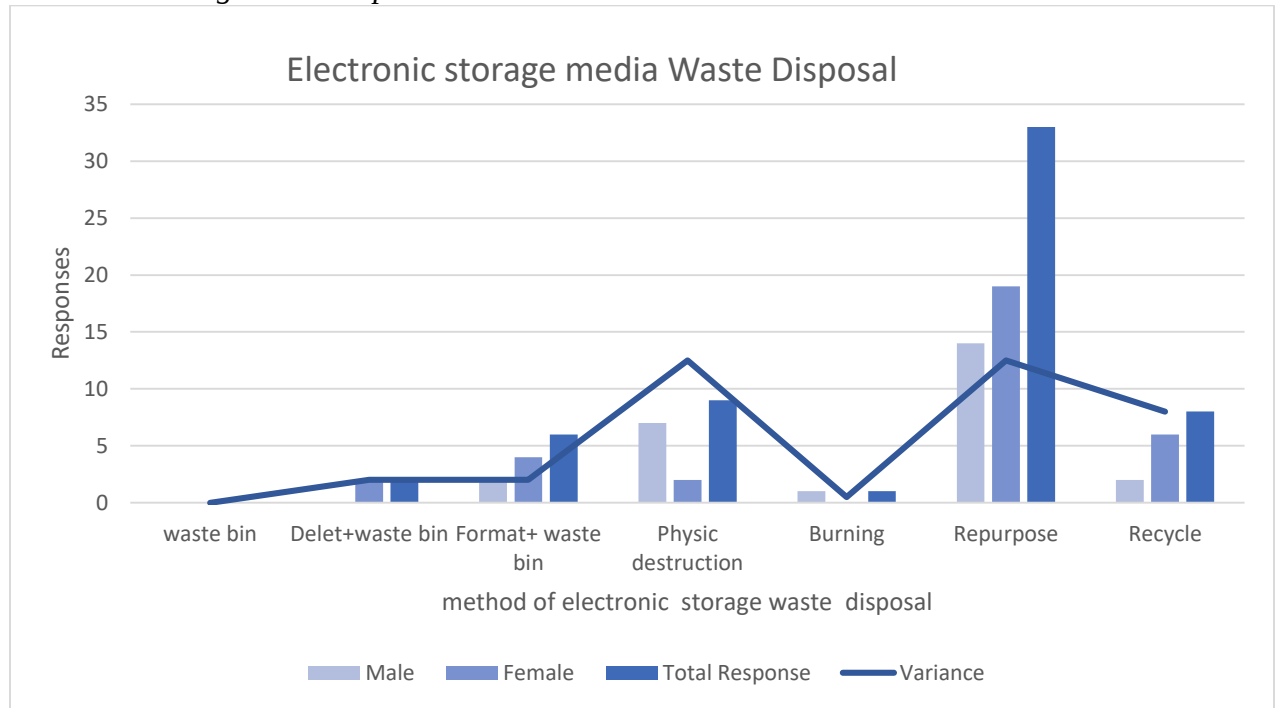
Table 4. 2

Electronic storage waste disposal

Electronic storage	Male	Female	Total response	Variance
Waste bin	0	0	0	0
Delet+waste bin	0	2	2	2
Format+ waste bin	2	4	6	2
Physic destruction	7	2	9	12.5
Burning	1	0	1	0.5
Repurpose	14	19	33	12.5
Recycle	2	6	8	8

Figure 4.2

Electronic storage waste disposal



From the table above it can be established that the majority of the staff 82.5% prefer to repurpose digital storage devices such as USB thumb drives and external storage such as memory cards and hard drives. This means that once a staff takes home a storage device such as a thumb drive without securely erasing it there is a risk that unauthorized individuals can access data storage. The risk is larger than that in printed papers because data in the storage device consist of complete actionable information and may be in larger quantity and variety compared to that on the one-page printed document. Personal use of the storage device also ensures more unauthorized people can easily access the content of the storage device with ease or even make a copy of the entire storage device. For a secure disposal of such devices which are burning at 2.5% and recycling at 5% constitute only 7.5%. This means staff linked to NLIMS chose the least secure option to dispose of storage

devices that may contain secure information. Female staff are more inclined to repurpose at 47.5% than male counterparts at 35%.

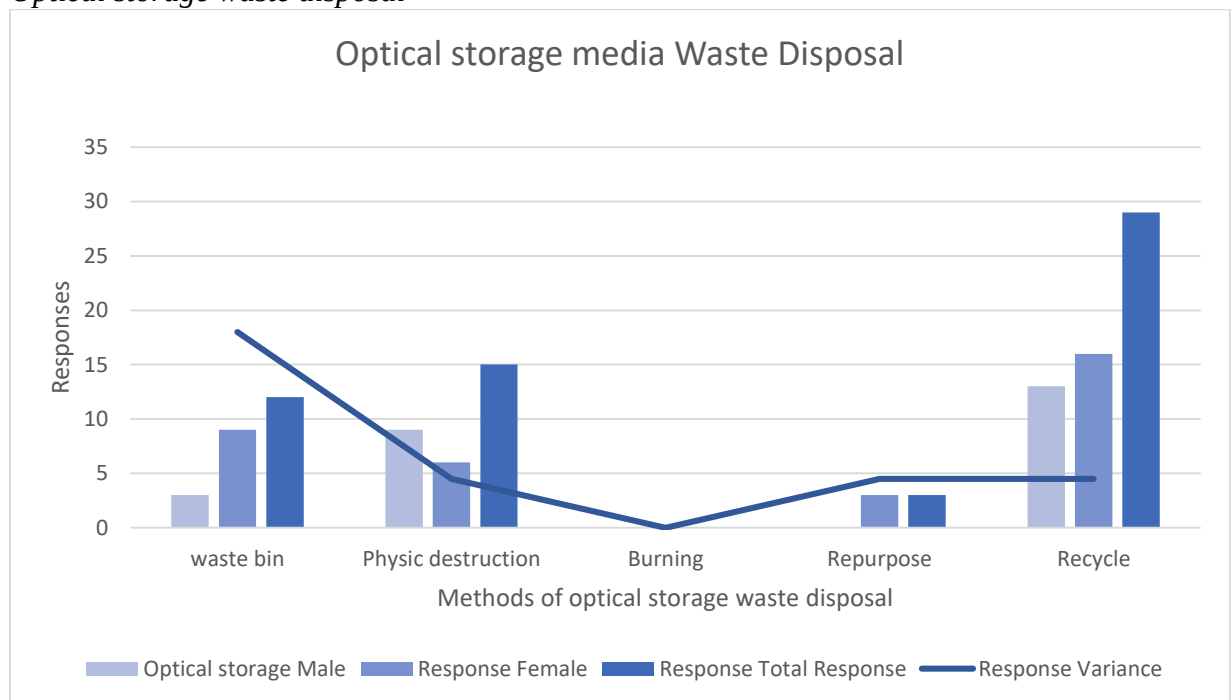
Table 4.3

Optical storage waste disposal

Ways to dispose	Male	Female	Total response	Variance
Waste bin	3	9	12	18
Physic destruction	9	9	15	4.5
Burning	0	0	0	0
Repurpose	10	3	3	4.5
Recycle	13	16	29	4.5

Figure 4.3

Optical storage waste disposal



Optical drives are an uncommon method of storage in the present time but were common ten years ago. In the attempt to digitalize all the NLIMS data some of the data stored in Optical drives were transferred into hard drives therefore, the optical drive may become

unnecessarily redundant. In this regard, many old optical disks were disposed of as waste. 72% of the respondents opted to recycle the disk. In this regard, disks are not physically destroyed as they go to be recycled and therefore, can be accessed by unauthorized individuals.

4.3.2 Working Station Privacy Shoulder Surfing

Table 4. 4

How shoulder surfing occurs in the workplace and home

Perpetrators	Response	Percentage
Senior staff	14	35
Workmate	9	22.5
Cleaning staff	3	7.5
Technician	9	22.5
Clients	3	7.5
Junior staff(intern)	7	17.5
Relatives	15	37.5

Figure 4.4

How shoulder surfing occurs in the workplace and home

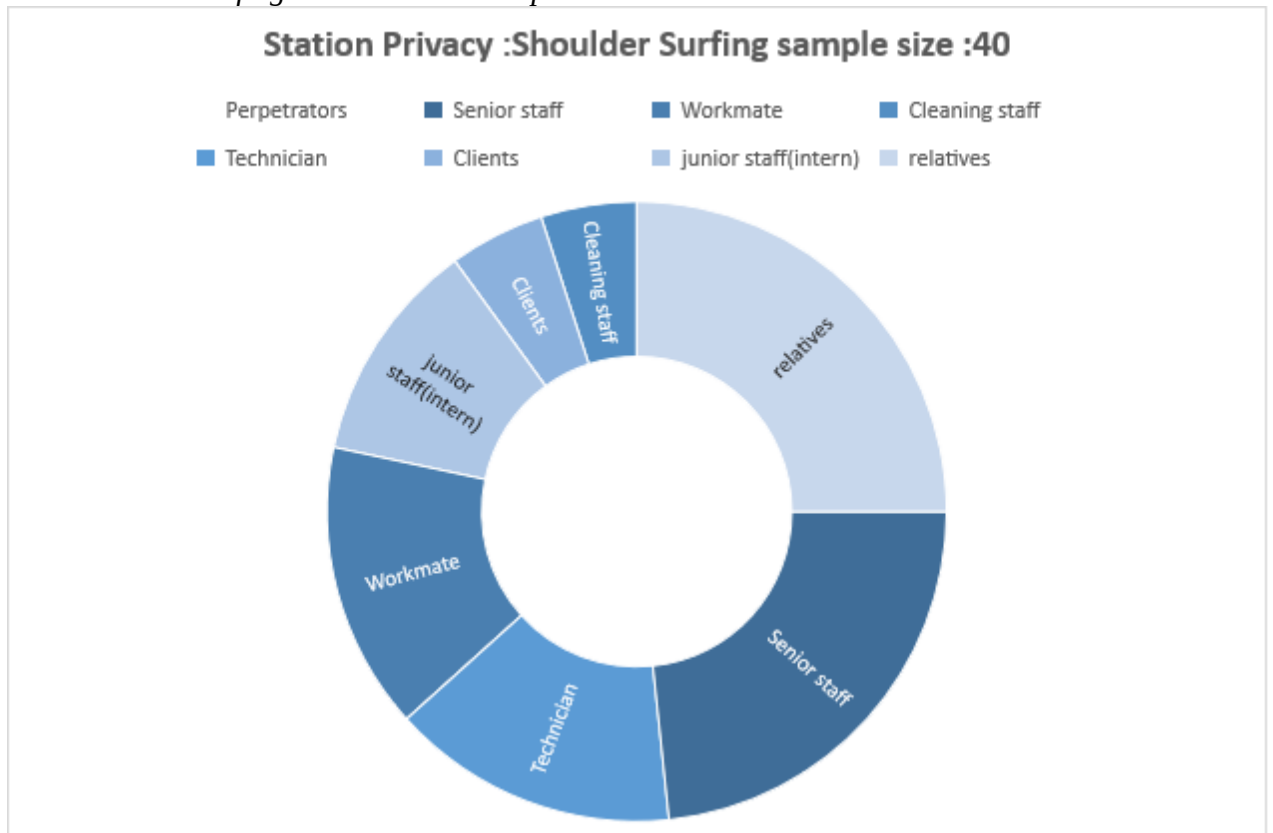
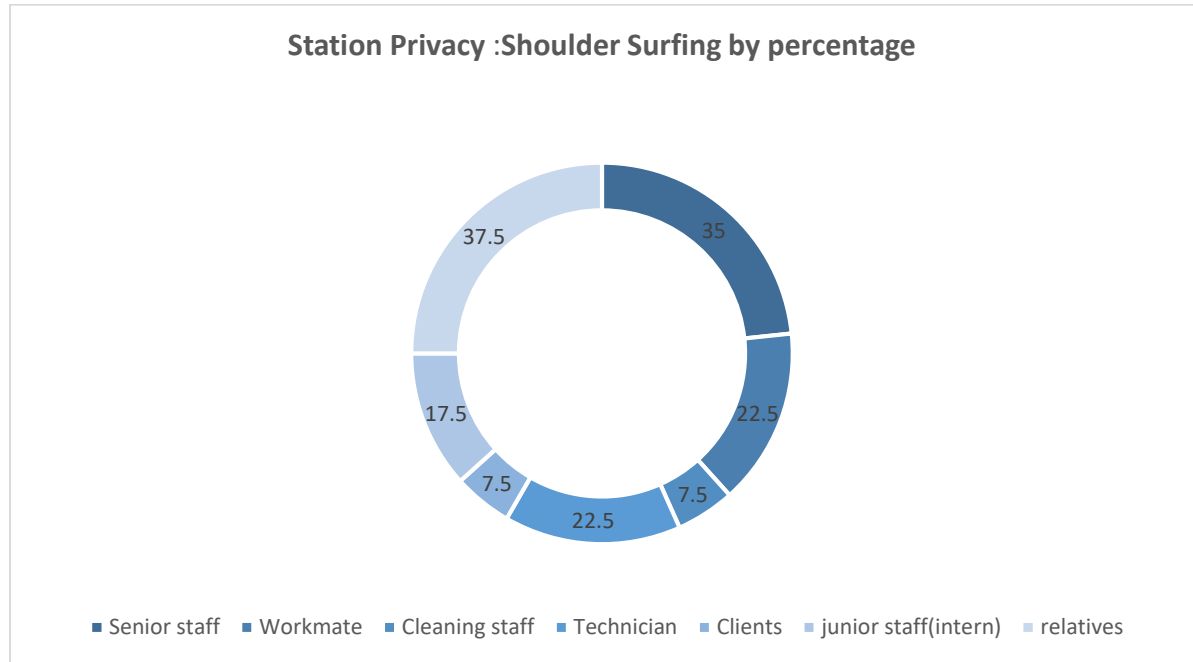


Figure 4.5

Station Privacy: Shoulder Surfing by percentage



Based on Table 4.4. up to 37.5% of NLIMS-linked staff agree that unauthorized personnel can access their computer through shoulder surfing. In comparison to the percentage of shoulder surfers who are staff, up to 35%, it shows more unauthorized people can access NLIMS information than those that are authorized through shoulder surfing.

4.3.3 Workstation Resource Sharing

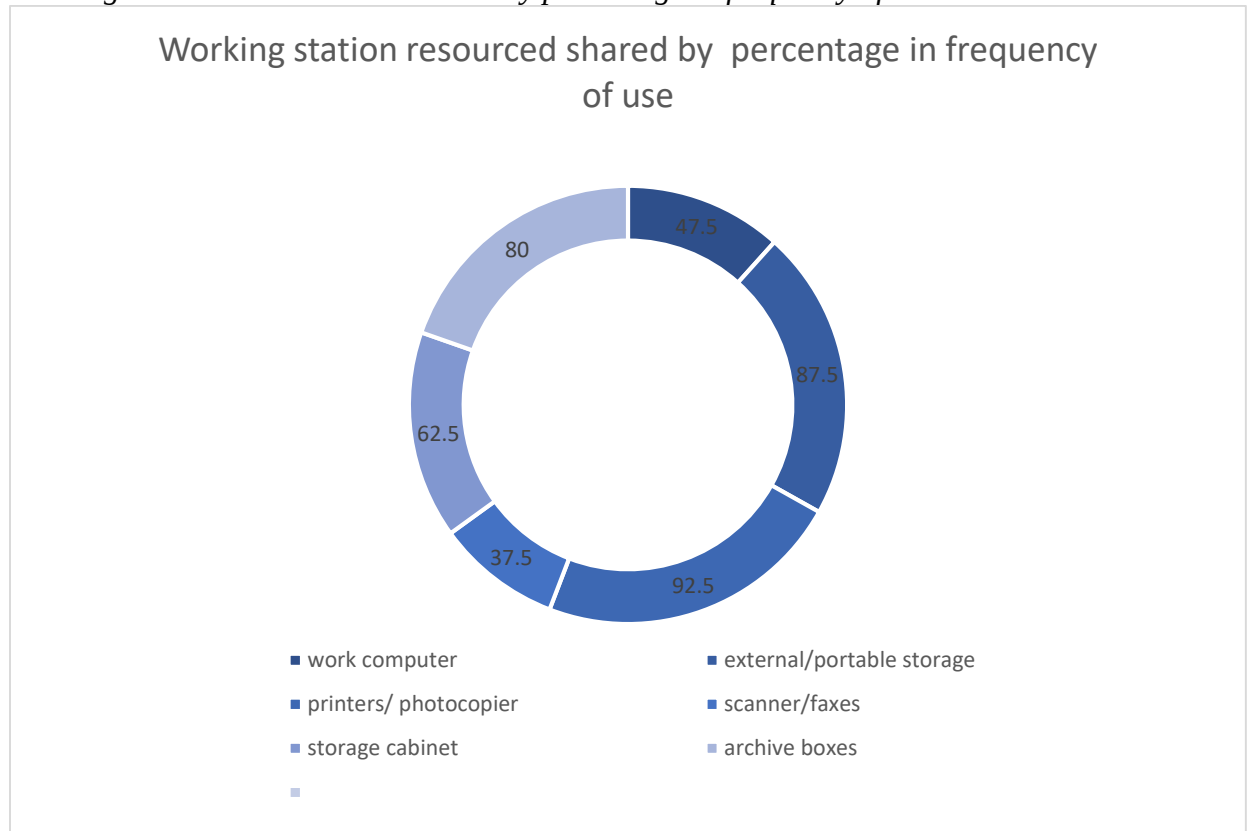
Table 4. 5

Workstation resource sharing

Resource	Response	Percentage
Working desktop	27	67.5
Work computer	19	47.5
External/portable storage	35	87.5
Printers/ photocopier	37	92.5
Scanner/faxes	15	37.5
Storage cabinet	25	62.5
Archives boxes	32	80.0

Figure 4.6

Working station resourced are shared by percentage in frequency of use.



Work pace resource sharing indicates the ability of other staff to access information from other staff that they may not be authorized to access. Access to work computer at 47.5%, external/portable storage at 87.5 and storage cabinet at 62.5% are direct access to actionable information by unauthorized staff which predisposes the NLIMS system data leakage. Cybercrime is not limited to non-staff but unfairly dismissed staff can leverage the easy access to information or the accessed information to sabotage the NLIMS system.

4.3.4 Social Engineering Awareness

Social engineering awareness test

Table 4.6*Social engineering awareness test sample size 40*

Social engineering awareness test sample size 40				
Section A ("YES" is the most desired answer)				
Question /statement	YES	NO	Don't Know	Maybe
Would you recognize if your personal computer is being hacked	13	19	2	6
Have you ever found a virus or Trojan on your personal computer?	17	3	12	8
Do you know how to tell if your computer has been hacked	1	29	7	3
Do you have knowledge of there having been a previous attack on your device	3	32	0	5
Do you know how to deal with it if there is an attack on your computer or a virus	9	27	3	1
Do you have knowledge about the cybercrime system	24	3	0	13
Is the firewall on your computer enabled?	13	0	19	8
Are you updating your operating system regularly?	4	27	0	9
Is the USB considered a transferor of viruses	23	0	0	17
Have you ever noticed someone you do not know or trust eavesdropping on your conversations, either over the phone or face-	9	17	0	14
Is there an anti-virus software on your device?	16	13	9	2
Are you updating your anti-virus software regularly?	4	32	4	0
Have you ever taken courses in social engineering?	3	33	0	4
Average	YES	NO	Don't Know	Maybe
	10.7	18.1	4.3	6.9
	7.7	13.0	5.9	5.3
Standard deviation				
Section B ("NO" is the most desired answer)				
	YES	NO	Don't Know	Maybe
Is the cost of the anti-virus program appropriate?	3	29	3	5
Attackers cannot target me; my computer has no value to them.	9	23	5	3
Have you used a public computer such as in the library or computer lab to log into your private information?	6	27	0	7
average	YES	NO	Don't Know	Maybe
	6.0	26.3	2.7	5.0
	3.0	3.1	2.5	2.0
Standard deviation				

Figure 4.7

Social engineering awareness test sample size 40: Section A

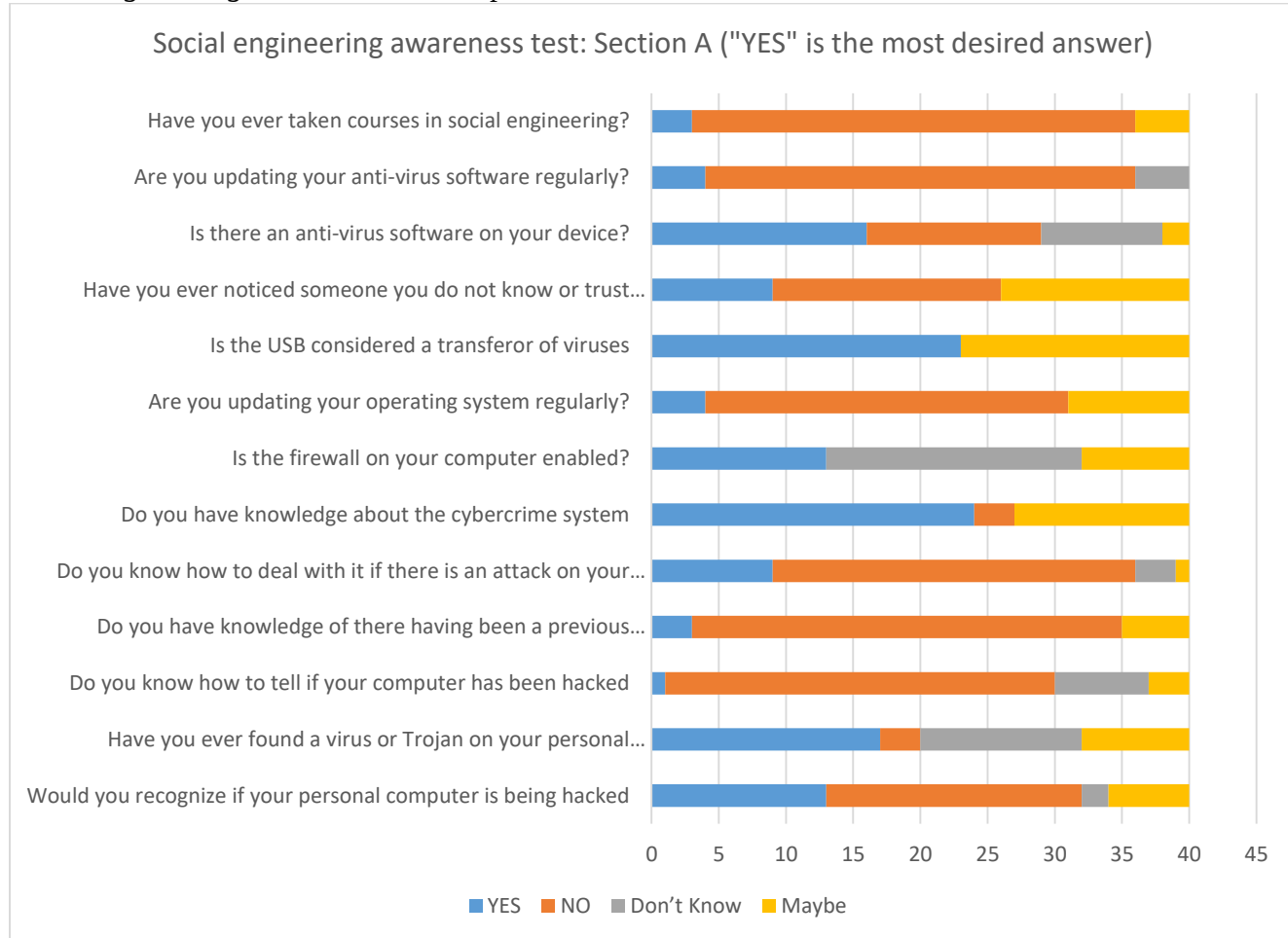


Figure 4.8

Social engineering awareness test sample size 40: Section A response summary

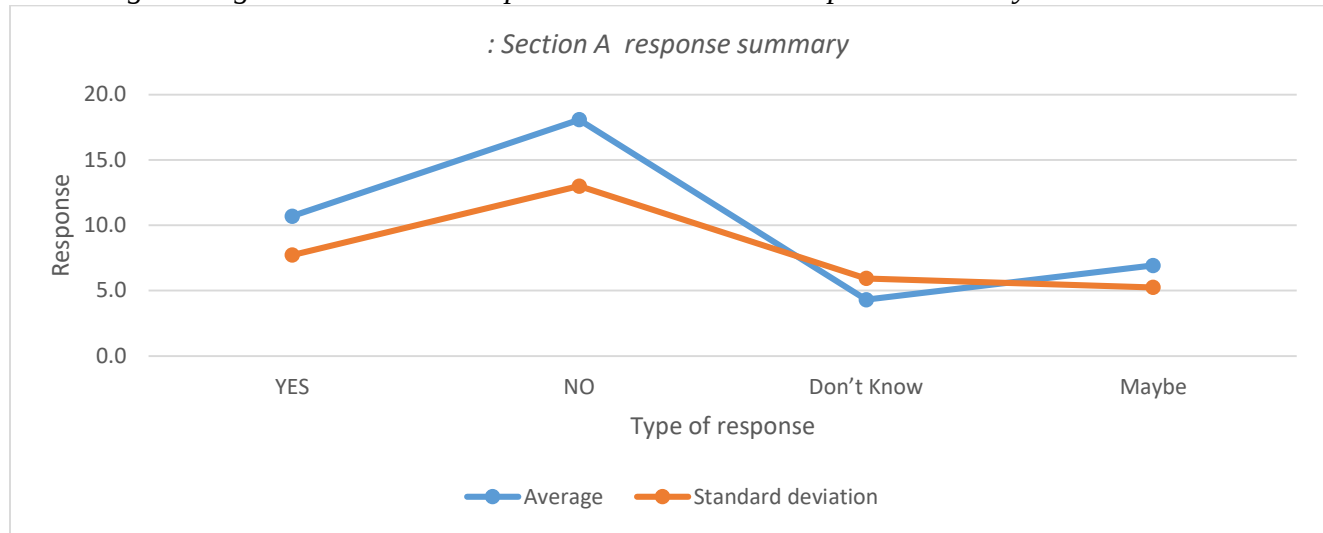


Figure 4.9

Social engineering awareness test sample size 40: Section B

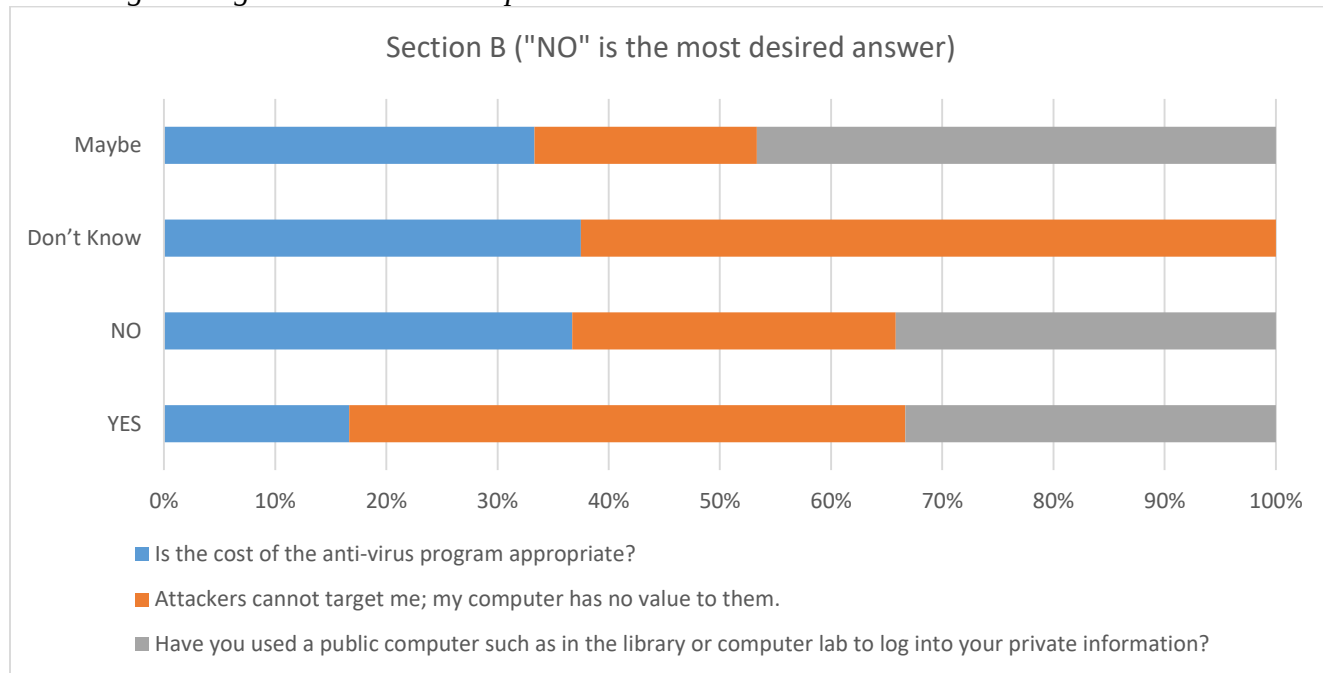
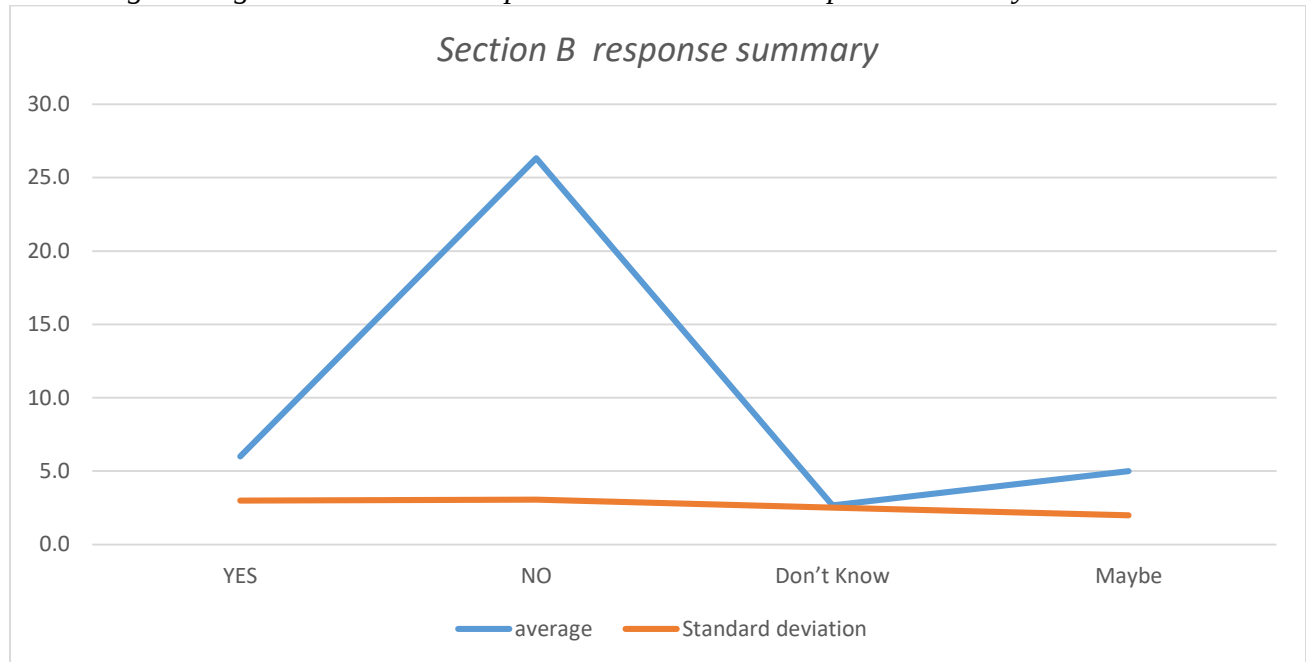


Figure 4.10

Social engineering awareness test sample size 40: Section B response summary



From Table 4.7, 18 out of 40 respondents 45% lack the knowledge, experience, and skills necessary to safeguard themselves against a social engineering attack. 17.3% are not sure if they are capable of avoiding preventing or stopping the attack. 10.75% do not know what social engineering is or what it is all about. In aggregate, 73% of the staff are incapable of securely protecting themselves against a social engineering attack.

4.4 Data Analysis

4.4.1 The status of shoulder surfing at NLIMS

This question seeks to establish whether NLIMS staff attempt to mitigate workstation privacy. Shoulder surfing offers unauthorized individuals an opportunity to access data from staff that can be used to infringe on information security at NLIMS. To answer this question two test factors were used to evaluate to what extent unauthorized personnel gain

access to information or data from the staff. The first test factor was the act of shoulder surfing and the second was workstation resource sharing.

4.4.2 Shoulder Surfing

The data for shoulder surfing was divided into two groups, one for perpetrators of shoulder surfing with access privileges such as key staff directly linked to the NLIMS system (not subordinates staff such as cleaners), and those without such as clients, relatives and interns. The ability to shoulder surf of the two groups was compared. The comparison is to establish if the level of access between the groups is significant. A t-test was conducted between the two groups. For this t-test a null hypothesis was used, the hypothesis states that; “There is no difference in the level of access between the two groups”.

Table 4. 7

t-test table derived from Table 4.4.: Workstation resource sharing, the following table Perpetrators

Individuals with access privileges	Response	Percentage
Senior staff	14	35.0
Workmate	9	22.5
Technician	9	22.5
Individuals without access privileges		
Clients	3	7.5
Junior staff(intern)	7	17.5
Relatives	15	37.5
Cleaning staff	3	7.5

Table 4.8*Descriptive statistical analysis of shoulder surfers*

<i>Authorised perpetrators</i>		<i>unauthorised perpetrators</i>	
Mean	26.66666667	Mean	20.83333333
Standard Error	4.166666667	Standard Error	8.819171037
Median	22.5	Median	17.5
Mode	22.5	Mode	#N/A
Standard Deviation	7.216878365	Standard Deviation	15.27525232
Sample Variance	52.08333333	Sample Variance	233.3333333
Kurtosis	#DIV/0!	Kurtosis	#DIV/0!
Skewness	1.732050808	Skewness	0.93521953
Range	12.5	Range	30
Minimum	22.5	Minimum	7.5
Maximum	35	Maximum	37.5
Sum	80	Sum	62.5
Count	3	Count	3
Confidence Level(95.0%)	17.92771971	Confidence Level(95.0%)	37.94583034

The actual descriptive table is attached to the appendix.

Table 4.9*t-test panel significance level of 0.05 or 5%**t-Test: Two-Sample Assuming Unequal Variances*

	<i>Authorized</i>	<i>Unauthorized</i>
Mean	26.66666666	20.83333333
Variance	52.08333333	233.3333333
Observations	3	3
Hypothesized Mean Difference	0	
t Stat	0.59805036	
P(T<=t) one-tail	0.29597226	
t Critical one-tail	2.35336343	
P(T<=t) two-tail	0.59194453	
t Critical two-tail	3.18244630	

The p-value of two-tail is 0.5913 rounded to 0.6 which is slightly greater than the significant acceptable value of 0.05. in this case, the null hypothesis that “There is no difference in the level of access between the two groups” is accepted indicating that the unauthorized perpetrators of shoulder surfers can shoulder surf at almost the same frequency as those that have access privileges.

Shoulder surfing majorly tested to what extent data or information accessed by NLIMS-linked staff can be accessible to those without access privileges especially those that are not linked in any way to the NLIMS system. Workstation resource sharing evaluates how easy it is for a coworker to access information or data from their coworker without permission through office shareable resources.

Table 4. 10*Workstation resource sharing sample 40 respondent*

Variables	Reliability of questionnaires from Trainees
Mean	27.14285714
Standard error	3.08937173
Median	27
Mode	N/A
Standard deviation	8.173709305
Sample variance	66.80952381
Kurtosis	-1.221367815
Skewness	-0.334486886
Range	22
Minimum	15
Maximum	37
Sum	190
Count	7
Confidence Level (95.0%)	7.559420299

According to Table 4.10: Workstation resource sharing, seven resources were cited. All of them have a 40% chance of a coworker accessing data or information that is not meant for them or that they do not have access to. What garbage disposal techniques are used to prevent dumpster diving? Descriptive analysis shows a mean of 27 which indicates that in aggregate.

Out of 40 respondents, 67.5 % agree that all the resources can be a source of the leak of vital data or information.

4.5 Summary

The findings indicated that the staff linked to the NLIMS system by at least 70% lacked the necessary knowledge on what is social engineering attack, how is it conducted, the

weakness that the attack relies on and the skills and experience to prevent or stop the attack. This data is further supported by findings on how the staff disposes of waste that may contain information or data that can be used to launch an attack on the said system. Findings also indicate that lower-rank staff access information that they are not authorized or cleared to access through the workstation resource-sharing policy.

4.6 Discussion of the Findings

4.6.1 The Status of Access to Controlled Information Through, Waste Disposal, Shoulder Surfing and Workstation Privacy.

In an information system, access to information or data is limited in the sense that the type of information determines who accesses it. Therefore, information that is regarded as critical to the integrity of the information system is highly limited with regard to accessibility. In aggregate information is categorized or classified and leads to the classification of accessibility, thus yielding a hierarchy of accessibility. Measures are usually put in place to protect the effectiveness of such a hierarchy. Some of these measures are effectively enforced in the technical area and some cases in the non-technical areas. Both areas need to be equally effective to deter any attack. In the case of NLIMS, the findings from this study indicate a degree of weaknesses in the non-technical area that may compromise the technical area. Analysis shows that waste disposal of material that may contain data and information on day-to-day operations in NLIMS is not effectively and securely disposed of to prevent unwanted access. Burning and physical destruction of such waste is done by very few staff leaving a large percentage of staff disposing of waste using methods that dumb star divers can exploit to launch attacks on the system.

The second area where the NLIMS system can be accessed is through shoulder surfing. This method is rather an innocent approach that is had to control in open office setup. In

an open office where staff formally and informally consult each other or engage in small office talk with their colleague, a staff be it junior or senior may access information on the desk of the other staff be it on the computer screen printed paper, on the phone screen, ongoing phone call, opened text message on the phone or short notes on an open notebook. Since this information is available for capture, anyone with malicious intent may devise methods and tactics to collect the information which they can use themselves or sell. Shoulder surfing can also happen at home when the staff carries their laptop at home. Shoulder surfing at home exposes the staff to more unauthorized people. This study analyzes the similarities in the frequency at which shoulder surfing occurs authorized – staff linked to NLIMS – and unauthorized people such as cleaners, relatives, and interns. It was established that the two groups could access the NLIMS system at the same frequency. This reveals that the NLIMS system is vulnerable to unauthorized individuals and the KMLPP is not employing precautions to limit external access to the system.

It is important to point out that cybercrime is not always from external sources but staff have been known to initiate the attack or help outsiders to launch an attack by providing internal information about the system only accessible to the staff. This leads to the third aspect of access control where through workstation resource sharing, information or data can be easily accessed by unauthorized staff. Findings have indicated that sharing storage cabinets, and external drives such as thumb drives or computers gives unauthorized staff access to information or data. These avenues are loopholes to access limited accessibility data or information that they are not cleared to access.

In aggregate, this study has sufficiently established that unsecured waste disposal, shoulder surfing, and unsecured resource sharing are non-technical weaknesses in KMLPP that can

be easily with limited effort exploited by individuals with malicious intent to attack the NLIMS system. It has also been established that available secure methods such as burning for waste disposal are being used by a minority of the staff at less than 20% leaving at least 70% to unsecured methods.

4.6.2 The Status of the Staff Knowledge of Social Engineering Attack

Social engineering is an approach that cybercriminals use to gather information on their target through the exploitation of the personal lifestyle of individuals. For many people they get attacked without knowing and vital information about them is stolen. Information collected through social engineering is usually sold to the highest bidder who can exploit it for a far larger and sinister attack. People directly linked to a critical information system such as NLIMS, are prime targets for social engineering. In this case, staff associated with or linked to NLIMS are expected to be well-equipped with knowledge and skills to prevent themselves from being victims of social engineering. Attack on such personnel can have far more dangerous ramifications.

Findings from this study have established that a large percentage of KMLPP staff linked to NLIMS are incapable of protecting themselves from a social engineering attack, it is further revealed that these percentages have not been formally trained or do not know what social engineering is. This current state of social engineering awareness for these staff recapitulates the poor choices in waste disposal and workstation privacy approaches.

4.6.3 The Status of the Effectiveness of the Non-Technical Approaches to Cyber Security Management at KMLPP NLIMS

After data analysis it has been established that the staff linked to the NLIMS system at least 70% lacked the necessary knowledge on what is social engineering attack, how is it

conducted, the weaknesses that the attack relies on, and the skills and experience to prevent or stop the attack. This data is further supported by findings on how the staff disposes of waste that may contain information or data that can be used to launch an attack on the said system. Findings also indicate that lower-rank staff access information that they are not authorized or cleared to access through the workstation resource-sharing policy. In this regard, the non-technical aspect of information security at KMLPP towards NLIMS has weaknesses that impair the overall effectiveness of the information security. About Holism's approach to cyber security posited by Gandhi, he propounds that despite complex barriers set up to deter cyber most often attackers still manage to break through (Gandhi, 2014). Gandhi, states that. "More often than not, computer break-ins are a collision of circumstances rather than a standalone vulnerability being exploited for a cyber-attack to succeed. In other words, it's the "whole" of the circumstances and actions of the attackers that cause the damage" (Gandhi, 2014). About KMLPP's weakness established by this study toward NLIMS, it is clear that KMLPP focuses more on the reductionist approach which strengthens the technical aspect of information security, and pays less attention to the holistic approach which factors in both technical and non-technical.

Most cyber security management approaches are based on a reductionist ideology (McLeod, 2008) this is focused on constituent parts of the system and the causality, as opined by Gandhi it has a robust practical use case. Under the lens of reductionist cyber security is approached from a specific point solution where attacks on known vulnerability can be anticipated (Gandhi, 2014). In the modern cyber system, there are systems such as human behavior and socio –cyber systems to mention a few that a reductionist approach is limited.

Social engineering attacks are highly mutable because they exploit people's lifestyles and thus their tricks and technic keep changing and cannot be predicted. There is therefore an inherent need for KMLPP.

To be adaptive in their approach to non-technical aspects of information security. This can be supported by Gandhi who suggests that a holistic approach to cyber security is analogous to the immunity of biological beings that are robust, adaptive, and constantly learning the ever-dynamic behavior of threats such as the mutation of a pathogen. With that in mind technical vulnerabilities which are human-based and influence cannot be effectively managed in the same way as technical vulnerabilities.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Summary

Access to information in an information system is limited, and the type of information determines who can access it. To protect the system's integrity, measures are put in place to categorize and classify information. In the case of NLIMS, weaknesses in non-technical areas have been identified, such as inadequate waste disposal, shoulder surfing, and unsecured resource sharing. These weaknesses can be exploited by individuals with malicious intent to attack the system. Waste disposal is done by a small percentage of staff, leaving a large percentage of staff disposing of waste using methods that hackers can exploit. Shoulder surfing occurs at home, exposing staff to more unauthorized individuals. The study found that authorized and unauthorized individuals can access the NLIMS system at the same frequency, indicating vulnerability to unauthorized individuals. Workstation resource sharing, such as storage cabinets and external drives, also allows unauthorized staff to access limited accessibility data. The study concludes that unsecured waste disposal, shoulder surfing, and unsecured resource sharing are non-technical weaknesses in KMLPP that can be exploited by malicious individuals.

Social engineering is a method used by cybercriminals to gather sensitive information about individuals, often leading to theft and larger attacks. This study reveals that a significant number of KMLPP staff linked to NLIMS are not adequately trained or aware of social engineering attacks. At least 70% of these staff lack knowledge about social engineering attacks, their conduct, and the skills to prevent or stop them. Additionally,

lower-rank staff access information they are not authorized to access through workstation resource-sharing policies. This non-technical aspect of information security at KMLPP towards NLIMS has weaknesses, impairing the overall effectiveness of the system. The study suggests that KMLPP's focus on a reductionist approach, which strengthens the technical aspect of information security, is less effective than a holistic approach that considers both technical and non-technical factors.

Cybersecurity management approaches often focus on reductionist ideologies, focusing on specific points of attack. However, in modern cyber systems, such as human behavior and socio-cyber systems, a reductionist approach is limited. Social engineering attacks are highly mutable, making it necessary for KMLPP to be adaptive in their approach to non-technical aspects. Gandhi suggests a holistic approach, analogous to the immunity of biological beings, to effectively manage non-technical vulnerabilities.

5.2 Conclusions

5.2.1 Objective one: The status of access to controlled information through, waste disposal, shoulder surfing, and workstation privacy

KMLPP uses measure shredding, and burning which are secure ways of disposing of material that may contain actionable data or information. The use of this method according to these studies, has established that they are not consistent throughout the staff sampled and they represent less than 20%. At least 70% use methods that are insecure. This study concludes that based on the data collected and analyzed, KMLPP does not pay enough attention to approaches to secure waste disposal which puts the NLIMS at risk of access to sensitive information through dumb star diving.

Concerning shoulder surfing, the study has found that unauthorized personnel can easily access information on staff computers or working desks. Based on this finding, the study concludes that a lower rank staff without link and access to the NLIMS information system can easily collect data and information through shoulder surfing.

On the subject of workstation privacy, this study has established that actionable information or data can be easily accessed by staff with lower security access due to the workstation resource-sharing policy. Therefore, the study concludes that staff with malicious intent can easily collect information or data by exploiting the workstation resource-sharing policy.

5.2.2 Objective two: The status of the staff knowledge of social engineering attack

This study has established that more than 60% of the sample respondents who are staff linked to NLIMS have no experience, skills, and knowledge to guard themselves against social engineering attacks. Based on this this study concludes that the majority of staff linked to NLIMS lack proper social engineering awareness.

5.2.3 Objective three: The status of the effectiveness of the non-technical approaches to cyber security management at KMLPP NLIMS.

Based on the four conclusions above this study in aggregate concludes that the non-technical approaches to cyber security at NLIMS are not effective in ever-evolving cybercrime tricks and tactics.

5.3 Recommendations

5.3.1 User Awareness and Training

There should be rigorous awareness and training in matters of cyber security specifically in ways staff can be a cyber-threat. This should be followed by training of the staff on

social engineering and measures and approaches they can use to protect themselves while online both at home and at work. Every new hire should be rigorously trained in NLIMS cyber security measures before admittance to matters and infrastructure linked to NLIMS

5.3.2 Policy Implementation

Policy change in the following areas is necessary in three areas. One, garbage disposal of any kind from employees linked to NLIMS should be proper whereby any information or data it carries in or on should be properly damaged beyond recovery. Garbage may include; printed material and storage devices. Second workstation etiquette should be strict in matters of shoulder surfing and officers should not leave unattended any material containing actionable data. Workstation computers should be off or users should log in when left unattended. Digital resource sharing should be managed under a secure platform and not through shareable storage media such as thumb drives. Thirdly staff should be restricted on the type of work resources they can take at home. Work-at-home cyber security guidelines should be revamped and strictly enforced to minimize information leaks to family members.

5.3.3 Communication and Collaboration

All strategies and policies that are designed to improve the information security in NLIMS should be properly communicated to every member and published and into medium and availed in platforms and places that ensure consistent reminder of the necessity of individual responsibility of every staff. This is meant to ensure collaboration and inspire collective effort to minimize social cyber security risks.

5.3.4 Risk Assessment and Management

Social cyber security is to be included as a major risk with high likelihood and severe consequences in the risk assessment and management department. This is to ensure sufficient resources, time, and attention is given to this subject. The aim to include it in a strategic cyber security approach that can be constantly be monitored, and assessed.

5.3.5 Continuous Monitoring and Improvement

This is critical and should be consistent because cyber threats evolve and as such installed measures and policies should be constantly tested and reviewed to ensure that they are capable of protecting the information system from the current threat. This task should be outsourced to a professional body to eliminate cases of bias or irrationality a social cyber security weakness.

5.4 Implications for Further studies

Benchmarking the implementation of a social-technical approach to cyber security is outside the scope of this study. For this study to successfully recommend this approach there is a need for an extensive further study to be done on the real-life application, success, and drawbacks of this social-technical approach.

REFERENCES

- Abdi, H., & Williams, L. J. (2010). Principal component analysis. *Wiley interdisciplinary reviews: computational statistics*, 2(4), 433-459.
https://wires.onlinelibrary.wiley.com/doi/abs/10.1002/wics.101?casa_token=vaty8oy80DUAAAAA%3AWm4ilxYmM2deY2Nbm5AC0Dt4TTf6bD_ZFTFu5srAFXfrH1dNEri12pZeMda3s9jpLnVoJ9TKdSu3_g
- Abrams, R. (2010, November 5). *Why is Unsecured WIFI So Risky?*
<http://blog.eset.com/2010/11/05/why-is-unsecured-wifi-so-risky>
- Aggarwal, P., Moisan, F., Gonzalez, C., & Dutt, V. (2018). Understanding cyber situational awareness in a cyber-security game involving recommendations. *International Journal on Cyber Situational Awareness*, 3(1), 29-38. <https://hal.science/hal-03188216/>
- Akhawe, D., & Felt, A. P. (2013). Alice in warningland: a {Large-Scale} field study of browser security warning effectiveness. In *22nd USENIX Security Symposium (USENIX Security 13)* (pp. 257-272).
<https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/akhawe>
- Alfawaz, S., May, L., & Mohannak, K. (2008). E-government security in developing countries: A managerial conceptual framework. In *Proceedings of the Twelfth Annual Conference of the International Research Society for Public Management (IRSPM 2008)* (pp. 1-14). Queensland University of Technology.
<https://eprints.qut.edu.au/18487/>
- Alsmadi, I. (2011). Security Challenges for Expanding E-governments' Services. *International Journal of Advanced Science and Technology*, 37, 47-60.
<https://d1wqtxts1xzle7.cloudfront.net/37627805/5-libre.pdf?1431580726=&response-content->
- Andrade, R. O., & Yoo, S. G. (2019). Cognitive security: A comprehensive study of cognitive science in cybersecurity. *Journal of Information Security and Applications*, 48, 102352.
<https://www.sciencedirect.com/science/article/abs/pii/S2214212618307804>

- Andrews, D. P. (1999). *National Security Telecommunications and Information Systems Security Committee. National Information Systems Security*. INFOSEC.
- Armstrong, R., Mayo, J., & Siebenlist, F. (2009). Complexity science challenges in cybersecurity. *Sandia National Laboratories SAND Report*.
<https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=ec5f02125bd83e8d0cb03a7d26e72575160199c3>
- Assange, J. (2006). *What is Wikileaks?* <http://wikileaks.org/>:
- Bahadur, G. (2012). *What is Social Media Insecurity?* http://www.siliconindia.com/guestcontributor/guestarticle/327/What_is_Social_Media_Insecurity_Gary_Bahadur.html
- Ataya, G., Cuypers, J., Steven, H. D., Guldentops, E., Hardy, G., Koning, G., et al. (2006). Enterprise Value: Governance of IT investment. *The Business Case*, 2-3.
https://www.researchgate.net/publication/309211305_VALIT_-_ING_Case_study
- Bell, G. (2001). Information Security Risk and Assessment. In *2001 UNC Charlotte Symposium on Information Security and Privacy*, <http://www.sis.uncc.edu/LIISP/slides01/Greg-Bell.pdf> (Accessed 28 April 2005).
<http://www.sis.uncc.edu/LIISP/slides01/Greg-Bell.pdf>
- Cacioppo, J. T., Petty, R. E., & Feng Kao, C. (1984). The efficient assessment of need for cognition. *Journal of personality assessment*, 48(3), 306-307.
https://www.tandfonline.com/doi/pdf/10.1207/s15327752jpa4803_13
- Chandler, A. (2017). The changing definition and image of hackers in popular discourse. In *Cyberspace Crime* (pp. 121-143). Routledge.
https://www.tandfonline.com/doi/pdf/10.1207/s15327752jpa4803_13https://www.taylorfrancis.com/chapters/edit/10.4324/9781315199627-8/changing-definition-image-hackers-popular-discourse-amanda-chandler
- Chen, H., & Yang, C. C. (Eds.). (2008). *Intelligence and security informatics: Techniques and applications* (Vol. 135). Springer Science & Business Media.
[https://books.google.co.ke/books?hl=en&lr=&id=LJ0R8wprgGgC&oi=fnd&pg=PR1&dq=Yang,+C.+\(2008\).+Intelligence+and+Security+Informatics+\(1+ed.\).+Springer&ots=o35rjz2dT8&sig=OM_mPGN5S_2Mjc7Dq3ymCcwCERQ&redir_esc=](https://books.google.co.ke/books?hl=en&lr=&id=LJ0R8wprgGgC&oi=fnd&pg=PR1&dq=Yang,+C.+(2008).+Intelligence+and+Security+Informatics+(1+ed.).+Springer&ots=o35rjz2dT8&sig=OM_mPGN5S_2Mjc7Dq3ymCcwCERQ&redir_esc=)

- y#v=onepage&q=Yang%2C%20C.%20(2008).%20Intelligence%20and%20Security%20Informatics%20(1%20ed.).%20Springer&f=false
- CISCO (2011, December 14). *Cisco Connected World Technology Report*.
<http://www.cisco.com/en/US/netsol/ns1120/index.html#~2011>
- Coleman, J. W. (2005). *The criminal elite: Understanding white-collar crime*. Macmillan.
- Conklin, A., & White, G. B. (2006, January). E-government and cyber security: the role of cyber security exercises. In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)* (Vol. 4, pp. 79b-79b). IEEE.
<https://ieeexplore.ieee.org/abstract/document/1579447>
- Frank, D. (2003). Policy would secure users, transactions. *Federal Computer Week, Falls Church, Jan, 27*, 10. <https://nap.nationalacademies.org/read/10685/chapter/5>
- Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *computers & security*, 31(8), 983-988.
<https://www.sciencedirect.com/science/article/abs/pii/S0167404812001228>
- Gandhi, G. (2014). *Complexity theory in Cyber Security*. University of Warwick.
- Gauci, M. (2008, October 23). Computer Literacy Required in Employment.
<http://www.infonet-ae.eu/en/news-items/computer-literacy-required-inemployment-0563>
- Global, N. (2023). *The Definitive Guide to IT Asset Disposal Security*. NCS Global.
- Grabosky, P., Smith, R., & Dempsey, G. (2001). *Electronic Theft: Unlawful Acquisition in Cyberspace*. Cambridge University Press.
- Haimes, Y. Y. (2009). On the definition of resilience in systems. *Risk Analysis: An International Journal*, 29(4), 498-501.
<https://web.p.ebscohost.com/ehost/detail/detail?vid=0&sid=22b01ba9-4367-4afd-95cc-8b508ee33330%40redis&bdata=JnNpdGU9ZWwhvc3QtbGl2ZQ%3d%3d>
- Hamid, S., & Madnick, S. (2016). Cyber safety: A systems theory approach to managing cyber security risks—Applied to TJX cyber-attack. *Work. Pap. CISL 2016*, 9.
- Hildick-Smith, A. (2005). Security for critical infrastructure scada systems. *SANS Reading Room, GSEC Practical Assignment, Version, 1*, 498-506.
<https://www.sans.org/white-papers/1644/>

- Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea. *Information & Management*, 49(2), 99-110. <https://www.sciencedirect.com/science/article/abs/pii/S0378720611001091>
- Humphreys, E. (2007). *Implementing the ISO/IEC 27001 information security management system standard*. Artech House, Inc. <https://dl.acm.org/doi/abs/10.5555/1543682>
- Hwang, M. S., Li, C. T., Shen, J. J., & Chu, Y. P. (2004). Challenges in e-government and security of information. *Information & Security*, 15(1), 9-20. https://procon.bg/system/files/15.01_Hwang_Li_%20Shen_Ch.pdf
- Jeffrey, J. T., & Joyce, R. B. P. (2012). On the Misuse of Slovin's Formula. *The Philippine Statistician*, 61(1), 129-36. https://www.psai.ph/docs/publications/tps/tps_2012_61_1_9.pdf
- Kaibiru, R. M., Karume, S. M., Kibas, F., & Onga'nyo, M. L. B. (2023). Closing the Cybersecurity Skill Gap in Kenya: Curriculum Interventions in Higher Education. *Journal of Information Security*, 14(2), 136-151. <https://www.scirp.org/journal/paperinformation?paperid=123376>
- Kanhere, V. (2009). IT Governance: Driving Value from Information Security: A Governance Perspective. *ISACA Journal*, 2, 15. <https://www.isaca.org/resources/news-and-trends/industry-news/2020/the-value-of-it-governance>
- Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business horizons*, 53(1), 59-68. <https://www.sciencedirect.com/science/article/abs/pii/S0007681309001232>
- Kash, W. (2012, June 5). Are Hackers Peering Through Your Laptop Webcam? <http://gov.aol.com/2012/06/05/are-hackers-peering-throughyour-laptop-webcam/>
- Keselman, H. J., Huberty, C. J., Lix, L. M., Olejnik, S., Cribbie, R. A., Donahue, B., ... & Levin, J. R. (1998). Statistical practices of educational researchers: An analysis of their ANOVA, MANOVA, and ANCOVA analyses. *Review of educational research*, 68(3), 350-386. <https://journals.sagepub.com/doi/abs/10.3102/00346543068003350>

- Kessler, K., Hettich, N., Parsons, C., Richardson, C., & Triana, A. (2011). A framework for assessing privacy readiness of e-Government. *Centre for Development Informatics, iGovernment Working Paper, 21*.
https://hummedia.manchester.ac.uk/institutes/gdi/publications/workingpapers/igov/igov_wp21.pdf
- Kinoti, K. (1998). *The ideological background to world population control: the quest for abundant life in Africa* Action Publishers
- Konstantinia, K., & Blyth, A. (2013). A socio-technical approach to cyber risk management and impact assessment. *ournal of Information Security, 4*, 33-41.
<http://dx.doi.org/10.4236/jis.2013.41005>
- Kothari, C. R. (2004). *Research Methodology: Methods and Techniques*. New Age International.
- Langenderfer, J., & Miyazaki, A. D. (2009). Privacy in the information economy. *Journal of Consumer Affairs, 43*(3), 380-388.
https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1745-6606.2009.01152.x?casa_token=BxX0q9KPZZ0AAAAA%3AuxKAeScWIxJbbth9dgBdLVxTlj0PC2A6xcWpL9Bqo8VKCnfZ85HNU3efAAAYbgzE9PQog1pfommdfPw
- Leveson, N. G. (2016). *Engineering a safer world: Systems thinking applied to safety* (p. 560). The MIT Press. <https://library.oapen.org/handle/20.500.12657/26043>
- Leveson, N. G. (2012). *A Systems-Theoretic View of Causality*. MIT Press.
<https://library.oapen.org/handle/20.500.12657/26043>
- Leveson, N. G. (2011). *A Systems-Theoretic View of Causality*. MIT Press
- Longe, O. B. (2004). *Proprietary Software Protection and Copyright issues in contemporary Information Technology* [Doctoral dissertation, Federal University of Technology, Akure].
<http://futaspace.futa.edu.ng:8080/xmlui/handle/123456789/898>
- Lukorito, G. M. (2012). *Information Security Threats And E-Government Initiatives*. University of Nairobi Press
- Madowo, L. (2011, January 4). *Hacker Defaces Website Of Kenya*.

- <http://techcrunch.com/2011/01/04/hacker-defaces-website-of-kenyapolice-in-tribute-of-mark-zuckerberg> Magigi, W. (2015). Research proposal development and report writing. *Pathway for Success in Higher Learning Institutions*. https://ilms.ifm.ac.tz/cgi-bin/koha/opac-detail.pl?biblionumber=16008&shelfbrowse_itemnumber=85699
- Makatiani, W. (2012). *Information Intelligence and Analytics*. <http://serianu.com>
- Mbuvi, D. (2012, January 17). *103 Government of Kenya websites were hacked overnight*. <http://www.cio.co.ke/news/main-stories/103-Government-of-Kenya-websites-hacked-overnight>
- Mikko, S. M., Pahnla, S., & Mahmood, A. (2007). Employees' adherence to information security policies: an empirical study. In *New Approaches for Security, Privacy and Trust in Complex Environments: Proceedings of the IFIP TC-11 22 nd International Information Security Conference (SEC 2007), 14–16 May 2007, Sandton, South Africa 22* (pp. 133-144). Springer US. https://link.springer.com/chapter/10.1007/978-0-387-72367-9_12
- Moore, D., Shannon, C., Brown, D. J., Voelker, G. M., & Savage, S. (2006). Inferring internet denial-of-service activity. *ACM Transactions on Computer Systems (TOCS)*, 24(2), 115-139. <https://dl.acm.org/doi/abs/10.1145/1132026.1132027>
- Morin, E. (1992). From the concept of system to the paradigm of complexity. *Journal of social and evolutionary systems*, 15(4), 371-385. <https://www.sciencedirect.com/science/article/abs/pii/1061736192900248>
- Mugenda, O. M., & Mugenda, A. G. (2003). *Research methods: quantitative and Qualitative approaches*. Acts Press.
- Ndombi, C. J. (2012). *Factors influencing performance of small and medium enterprises in Bungoma South District, Kenya* [Doctoral dissertation, University of Nairobi, Kenya]. Kenya. <http://erepository.uonbi.ac.ke/handle/11295/8221>
- Nikkhahan, B., Aghdam, A. J., & Sohrabi, S. (2009). E-government security: A honeynet approach. *International Journal of Advanced Science and Technology*, 5, 75-84. <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=ccee89b9dd8639671e03f0159a7ad1dc6e88e48f>

- Niraula, S. R. (2019). A review of research process, data collection and analysis. *Insights in Biology and Medicine*, 3(1), 001-006.
<https://www.biologymedjournal.com/abstract/ibm-aid1014>
- Norman, D. (2022). *Socio-Technical Systems*. Interaction Design Foundation.
<https://www.interaction-design.org/literature/topics/socio-technical-systems>
- Oliver, D., Allard, J.-L., Antonsson, E., Bahl, S., Brotby, K. W., & Dimitriadis, C. (2009). *The business model for information security*. ISACA.
- Omwansa, T. (2009). M-PESA: Progress and prospects. *Innovations*, 107, 475.
https://d1wqtxts1xzle7.cloudfront.net/87040674/innov-gsma-omwansa-libre.pdf?1654464218=&response-content-disposition=inline%3B+filename%-IS-oOo2CGc20pN2Z2D8-Uw5ZujbdhR4WTYiFoX~Q__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA
- Orodho, J. A. (2005). *Elements of Education and social science research methods*. University of Nairobi Press.
- Prashat, K., & Bhalerao, S. (2010). Sample size calculation. *International journal of Ayurveda research*, 1(1), 55.
<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2876926/>
- Puhakainen, P. (2006). *A design theory for information security awareness*.
<https://oulurepo.oulu.fi/handle/10024/35491>
- Rangwala, H. (2022). *Socio-technical Systems*. Geeks for Geeks.
- Salim, H., & Madnick, S. (2016). Cyber safety: A systems theory approach to managing cyber security risks–Applied to TJX cyber-attack. *Work. Pap. CISL 2016*, 9.
- Sang, H., Kim, S. H., Yang, K. H., & Park, S. (2014). An integrative behavioral model of information security policy compliance. *The Scientific World Journal*, 2014(1), 463870. <https://onlinelibrary.wiley.com/doi/full/10.1155/2014/463870>
- Savage, S., & Schneider, F. B. (2009). *Cybersecurity*.
<http://www.cra.org/ccc/files/docs/init/Cybersecurity.pdf>.
- Schneier, B. (2015). *Secrets and lies: digital security in a networked world*. John Wiley & Sons.
[https://books.google.co.ke/books?hl=en&lr=&id=OT6kBgAAQBAJ&oi=fnd&pg=PR9&dq=Schneier,+B.+\(2004\).+Secrets+and+Lies:+Digital+Security+in+a+Net](https://books.google.co.ke/books?hl=en&lr=&id=OT6kBgAAQBAJ&oi=fnd&pg=PR9&dq=Schneier,+B.+(2004).+Secrets+and+Lies:+Digital+Security+in+a+Net)

worked+World.+Wiley.&ots=N6s-PFmV2I&sig=9-jWx7sFeNZg7e7bAumwJ-C7NcQ&redir_esc=y#v=onepage&q&f=false

- Scott, R. (2003). *Planners need to plan for disaster*. Accounting Today
- Sembok, T. T. (2003). *Ethics of Information Communication Technology (ICT)*. Universiti Kebangsaan Bangkok.
- Singh, A. S., & Masuku, M. B. (2014). Sampling techniques & determination of sample size in applied statistics research: An overview. *International Journal of economics, commerce and management*, 2(11), 1-22.
https://d1wqtxts1xzle7.cloudfront.net/65225177/21131_IJECM-libre.pdf?1608404466=&response-content-Id=APKAJLOHF5GGSLRBV4ZA
- Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information management & computer security*, 8(1), 31-41.
https://www.emerald.com/insight/content/doi/10.1108/09685220010371394/full.html?casa_token=ldqYOVnocUIAAAAA:-DKUkXksl7brAEJJoQ_IOaBACntTaSxUztLOBc3_eHyYzczAPHKMrDTPv8HlrjroWc521Uir2Dl65CAq_GMW2FAJ9EH5sp_krz_3Jletgruy5i2H4q8
- Smith, S., & Jamieson, R. (2006). Determining key factors in e-government information system security. *Information systems management*, 23(2), 1-9.
<https://www.tandfonline.com/doi/pdf/10.1201/1078.10580530/45925.23.2.20060301/92671.4>
- Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & security*, 24(2), 124-133.
<https://www.sciencedirect.com/science/article/abs/pii/S0167404804001841>
- Stephan, S., Magigi, W., & Godfrey, B. (2015). The organization of urban agriculture: Farmer associations and urbanization in Tanzania. *Cities*, 42, 153-159.
<https://www.sciencedirect.com/science/article/abs/pii/S0264275114000882>
- Stibbe, M. (2005). *E-government security*. Infosecurity Today
- Veksler, V. D., Buchler, N., Hoffman, B. E., Cassenti, D. N., Sample, C., & Sugrim, S. (2018). Simulations in cyber-security: a review of cognitive modeling of network attackers, defenders, and users. *Frontiers in psychology*, 9, 691.

<https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2018.00691/full>

- Wanjiru, W. E., & Kimutai, G. (2013). Determinants of effective monitoring and evaluation systems in non-governmental organizations within Nairobi County, Kenya [Master's thesis, Kenyatta University]. Kenya. <https://d1wqtxts1xzle7.cloudfront.net/75323323>
- Wendy, H. M. (2022). *Complexity Theory*. [https://Complexity Theory - strategy, organization, levels, system, manager, company, business, system \(referenceforbusiness.com\)](https://Complexity Theory - strategy, organization, levels, system, manager, company, business, system (referenceforbusiness.com))
- West, R. (2008). The psychology of security. *Communications of the ACM*, 51(4), 34-40. <https://dl.acm.org/doi/fullHtml/10.1145/1330311.1330320>
- Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual differences in cyber security behaviors: an examination of who is sharing passwords. *Cyberpsychology, Behavior, and Social Networking*, 18(1), 3-7. <https://www.liebertpub.com/doi/full/10.1089/cyber.2014.0179>
- Wiederhold, B. K. (2014). The role of psychology in enhancing cybersecurity. *Cyberpsychology, Behavior & Social Networking*, 17(3), 131-132. <https://web.p.ebscohost.com/ehost/detail/detail?vid=0&sid=b3cd837a-a9df-4c4d-be63-ccd34e46c778%40redis&bdata=JnNpdGU9ZWWhvc3QtbGl2ZQ%3d%3d#AN=94756994&db=a9h>
- Wilner, A. (2017). Cyber deterrence and critical-infrastructure protection: Expectation, application, and limitation. *Comparative Strategy*, 36(4), 309-318. https://www.tandfonline.com/doi/abs/10.1080/01495933.2017.1361202?casa_token=sdlpGJy2B8UAAAAA:ZoDPLACAT31quIOmR2vrOQVJgznDXJ-RPEEaHk4ij-BHK7F8rVQd-0F2rks10-If-1aiK9jwJcCi7Qk
- Yar, M. (2006). *Cybercrime and Society*. SAGE Publications Ltd.

APPENDICES

Appendix I: Descriptive statistical analysis of shoulder surfers

<i>Authorized perpetrators</i>			<i>unauthorized perpetrators</i>	
Mean	26.66666667		Mean	20.83333333
Standard Error	4.166666667		Standard Error	8.819171037
Median	22.5		Median	17.5
Mode	22.5		Mode	#N/A
Standard Deviation	7.216878365		Standard Deviation	15.27525232
Sample Variance	52.08333333		Sample Variance	233.3333333
Kurtosis	#DIV/0!		Kurtosis	#DIV/0!
Skewness	1.732050808		Skewness	0.93521953
Range	12.5		Range	30
Minimum	22.5		Minimum	7.5
Maximum	35		Maximum	37.5
Sum	80		Sum	62.5
Count	3		Count	3
Confidence Level(95.0%)	17.92771971		Confidence Level(95.0%)	37.94583034

Appendix II: Consent to Participate in the Study

UNIVERSITY NAME: KENYA METHODIST UNIVERSITY.

RESEARCH TITLE: ASSESSMENT OF THE EFFECTIVENESS OF NON-TECHNICAL APPROACH TO CYBER SECURITY MANAGEMENT FOR KENYA MINISTRY OF LANDS AND PHYSICAL PLANNING NLIMS SYSTEM.

CONSENT FORM

RESEARCHERS NAME Gabriel Ndung'u

.....
.....

Voluntary Participation. You are being offered the opportunity to participate in a research study. At all times, you have the right to be informed about the study procedures so that you can decide whether you want to consent to participation. At all times, please feel free to ask the Researcher to explain any information that you do not understand or for which you would like additional information. Your participation in this study is entirely voluntary. You do not have to be involved in the Study if you do not want to. You may refuse or decline participation in the Study at any time (including before and after you sign this Consent), and nothing adverse will happen to you. If you do not want to continue to be involved in the Study, you may stop at any time without penalty or loss of any compensation or other benefits to which you are otherwise entitled. Please contact the Researcher identified above at any time if you have any questions, comments, or concerns.

Confidentiality. By participating in the Study, the Participant may become privy to, or otherwise observe or learn about confidential information related to the subject matter of the Study and/or Researcher's work (hereinafter collectively, the "Confidential Information"). Participant agrees that except for disclosures required by applicable law, and information which is a matter of public record, Participant shall not, during the term

of the Study or any time after the conclusion of the Study, disclose any Confidential Information to any person or use any Confidential Information for the benefit of Participant or any other person, except with the prior written consent of the Researcher.

IN WITNESS WHEREOF, the undersigned executes this Informed Consent to Participate in the Research Study as of the date indicated below.

Last Name:

First Name:

Middle Name.....

Date..... Sign.....

Appendix III: Questionnaire

My name is **Gabriel Ndung'u**. Am conducting a study on the **ASSESSMENT OF THE EFFECTIVENESS OF a NON-TECHNICAL APPROACH TO CYBER SECURITY MANAGEMENT FOR the KENYA MINISTRY OF LANDS AND PHYSICAL PLANNING NLIMS SYSTEM**.

I am pleased to notify you that you have been chosen to participate in this research. I'd like to ask for your help in filling out the enclosed questionnaire, which is an important part of the study process. Please provide the most correct answers to the following questions. Your response was kept completely private and anonymous. The responses are only to be used for academic purposes. Please check the appropriate box ☐ to answer the following questions.

1. Station Privacy

a) Shoulder surfing

Instructions: Please tick inside the check box

Perpetrators	response
Senior staff	☐ Check
Workmate	☐ Check
Cleaning staff	☐ Check
Technician	☐ Check
Clients	☐ Check
Junior staff(intern)	☐ Check
Relatives	☐ Check

b) Station resource sharing

Resource shared	response
working desktop	☐ Check
work computer	☐ Check
external/portable storage	☐ Check
printers/ photocopier	☐ Check
scanner/faxes	☐ Check
storage cabinet	☐ Check
archive boxes	☐ Check

2. Access control

a) Storage media Waste Disposal

i. *Electronic storage*

Ways to dispose	response
waste bin	☐ Check
Delet+waste bin	☐ Check
Format+ waste bin	☐ Check
Physic destruction	☐ Check
Burning	☐ Check
Repurpose	☐ Check
Recycle	☐ Check

ii. *Optical storage*

Ways to dispose	response
waste bin	☐ Check
Physic destruction	☐ Check
Burning	☐ Check
Repurpose	☐ Check
Recycle	☐ Check

b) Printed document waste disposal

Ways to dispose	response
Waste bin	☐ Check
Waste bin+ Recycle	☐ Check
Shredding + waste bin	☐ Check
burning	☐ Check
Repurpose/Reuse	☐ Check

3. Social engineering awareness

Instructions: make all the choices with 1 where you agree and 0 where you don't. Note, mark all the choices.

Social engineering awareness test				
Section A ("YES" is the most desired answer)				
Question /statement	YES	NO	Don't Know	Maybe
Would you recognize if your personal computer is being hacked?				
Have you ever found a virus or Trojan on your personal computer?				
Do you know how to tell if your computer has been hacked?				
Do you know there has been a previous attack on your device?				
Do you know how to deal with it if there is an attack on your computer or a virus?				
Do you know the cybercrime system?				
Is the firewall on your computer enabled?				
Are you updating your operating system regularly?				
Is the USB considered a transferor of viruses				
Have you ever noticed someone you do not know or trust eavesdropping on your conversations, either over the phone or face-to-face conversations? Yes				
Is there an anti-virus software on your device?				
Are you updating your anti-virus software regularly?				
Have you ever taken courses in social engineering?				
Section B ("NO" is the most desired answer)	YES	NO	Don't Know	Maybe
Is the cost of the anti-virus program appropriate?				
Attackers cannot target me; my computer has no value to them.				

Have you used a public computer such as in the library or computer lab to log into your private information?				
--	--	--	--	--

Appendix IV: Research confirmation letter from Director of Postgraduate studies



KENYA METHODIST UNIVERSITY

P. O. Box 267 Meru - 60200, Kenya
Tel: 254-064-30301/31229/30367/31171

Fax: 254-64-30162
Email: deanrd@kemu.ac.ke

DIRECTORATE OF POSTGRADUATE STUDIES

November 1, 2022

Commission Secretary,
National Commission for Science, Technology and Innovations,
P.O. Box 30623-00100,
NAIROBI.

Dear Sir/Madam,

RE: GABRIEL NDUNG'U – (REG. NO. CIS-3-2653-2/2014)

This is to confirm that the above named is a bona fide student of Kenya Methodist University, in the School of Science and Technology, Department of Computer Science undertaking a Masters' Degree in Computer Science. He is conducting research on: "A Socio-Technical Assessment Tool on the Effectiveness of Non-Technical Cyber Security Management for Kenya Ministry of Lands and Physical Planning NLIMS System".

We confirm that his research proposal has been presented and approved by the University.

In this regard, we are requesting your office to issue a research license to enable him collect data.

Any assistance accorded to him will be appreciated.

Thank you.


Dr. John Muchiri (PhD)
Director, Postgraduate Studies

Cc: Dean SST
CoD, CS
Postgraduate Co-ordinator - CS
Student Supervisors

Appendix I: NACOSTI Research Permit

 REPUBLIC OF KENYA	 NATIONAL COMMISSION FOR SCIENCE, TECHNOLOGY & INNOVATION
Ref No: 217077	Date of Issue: 14/November/2022
RESEARCH LICENSE	
	
This is to Certify that Mr., Gabriel Ndung'u of Kenya Methodist University, has been licensed to conduct research as per the provision of the Science, Technology and Innovation Act, 2013 (Rev.2014) in Nairobi on the topic: A SOCIO-TECHNICAL ASSESSMENT TOOL ON THE EFFECTIVENESS OF NON-TECHNICAL CYBER SECURITY MANAGEMENT FOR KENYA MINISTRY OF LANDS AND PHYSICAL PLANNING NLIMS SYSTEM for the period ending : 14/November/2023.	
License No: NACOSTI/P/22/21949	
217077	
Applicant Identification Number	Director General
	NATIONAL COMMISSION FOR SCIENCE, TECHNOLOGY & INNOVATION
	Verification QR Code
	
NOTE: This is a computer generated License. To verify the authenticity of this document, Scan the QR Code using QR scanner application.	
See overleaf for conditions	

THE SCIENCE, TECHNOLOGY AND INNOVATION ACT, 2013 (Rev. 2014)
Legal Notice No. 108: The Science, Technology and Innovation (Research Licensing)
Regulations, 2014

The National Commission for Science, Technology and Innovation, hereafter referred to as the Commission, was established under the Science, Technology and Innovation Act 2013 (Revised 2014) herein after referred to as the Act. The objective of the Commission shall be to regulate and assure quality in the science, technology and innovation sector and advise the Government in matters related thereto.

CONDITIONS OF THE RESEARCH LICENSE

1. The License is granted subject to provisions of the Constitution of Kenya, the Science, Technology and Innovation Act, and other relevant laws, policies and regulations. Accordingly, the licensee shall adhere to such procedures, standards, code of ethics and guidelines as may be prescribed by regulations made under the Act, or prescribed by provisions of International treaties of which Kenya is a signatory to
2. The research and its related activities as well as outcomes shall be beneficial to the country and shall not in any way;
 - i. Endanger national security
 - ii. Adversely affect the lives of Kenyans
 - iii. Be in contravention of Kenya's international obligations including Biological Weapons Convention (BWC), Comprehensive Nuclear-Test-Ban Treaty Organization (CTBTO), Chemical, Biological, Radiological and Nuclear (CBRN).
 - iv. Result in exploitation of intellectual property rights of communities in Kenya
 - v. Adversely affect the environment
 - vi. Adversely affect the rights of communities
 - vii. Endanger public safety and national cohesion
 - viii. Plagiarize someone else's work
3. The License is valid for the proposed research, location and specified period.
4. The license any rights thereunder are non-transferable
5. The Commission reserves the right to cancel the research at any time during the research period if in the opinion of the Commission the research is not implemented in conformity with the provisions of the Act or any other written law.
6. The Licensee shall inform the relevant County Director of Education, County Commissioner and County Governor before commencement of the research.
7. Excavation, filming, movement, and collection of specimens are subject to further necessary clearance from relevant Government Agencies.
8. The License does not give authority to transfer research materials.

9. The Commission may monitor and evaluate the licensed research project for the purpose of assessing and evaluating compliance with the conditions of the License.
10. The Licensee shall submit one hard copy, and upload a soft copy of their final report (thesis) onto a platform designated by the Commission within one year of completion of the research.
11. The Commission reserves the right to modify the conditions of the License including cancellation without prior notice.
12. Research, findings and information regarding research systems shall be stored or disseminated, utilized or applied in such a manner as may be prescribed by the Commission from time to time.
13. The Licensee shall disclose to the Commission, the relevant Institutional Scientific and Ethical Review Committee, and the relevant national agencies any inventions and discoveries that are of National strategic importance.
14. The Commission shall have powers to acquire from any person the right in, or to, any scientific innovation, invention or patent of strategic importance to the country.
15. Relevant Institutional Scientific and Ethical Review Committee shall monitor and evaluate the research periodically, and make a report of its findings to the Commission for necessary action.

National Commission for Science, Technology and
Innovation(NACOSTI),
Off Waiyaki Way, Upper Kabete,
P. O. Box 30623 - 00100 Nairobi, KENYA
Telephone: 020 4007000, 0713788787, 0735404245
E-mail: dg@nacosti.go.ke
Website: www.nacosti.go.ke