FACTOR THAT CONTRIBUTES INFORMATION SECURITY VULNERABILITIES IN PUBLIC ORGANIZATION: A CASE OF TEMDO AND TAEC – ARUSHA

NELSON BYSON MISHETO

MBA (Masters of Information Technology Management)

Institute of Accountancy Arusha

November, 2020

FACTORS THAT CONTRIBUTE INFORMATION SECURITY VULNERABILITIES IN PUBLIC ORGANIZATION: A CASE OF TEMDO AND TAEC - ARUSHA

BY
NELSON BRYSON MISHETO

NOVEMBER, 2020

This work contained within this document has been submitted by the student in partial fulfilment of Master of Information Technology Management

CERTIFICATION

I, the undersigned certify that I have read and hereby recommend for acceptance by Institute of Accountancy the dissertation entitled: Factors that contribute information security vulnerabilities in public entities: A case of TEMDO and TAEC - Arusha in fulfilment of the requirements for the degree of Master of Information Technology Management offered at the Institute of Accountancy Arusha.

……………………………………………….

(Supervisor Signature)

…………………………………………………

(Supervisor Name)

Date ………………………………

DECLARATION

I, Nelson Bryson Misheto, declare that this dissertation is my own original work and that it has not been presented and will not be presented to any university for similar or any other degree award.

Signature…………………………………………

Date…………………………………..

DEDICATION

I dedicate this work to my brother and sister as well as my lovely Mom.

ACKNOWLEDGEMENTS

Special thanks to the Almighty God for his love and providence and for giving me wisdom to accomplish this work. I wish to express my sincere appreciation to my supervisor Dr. Kiwango for his professional guidance throughout my research proposal. I wish to acknowledge the effort of my family for their extreme moral support, encouragement and patience during the course of studies as well as throughout my academic career. Special thanks to my colleagues who assisted me in getting materials for my research. Finally, I extend special thanks to all those who have contributed at various stages of this proposal to make it a success. God bless you all.

ABSTRACT

The study sought to investigate factors that contribute information security vulnerabilities in public organizations: A case of TEMDO and TAEC - Arusha. The study established the external organizational factors that may contribute to information security vulnerabilities in public organizations. The study also determined internal organizational factors that may contribute to information security vulnerabilities in public organizations. Descriptive cross-sectional survey research design was useful for collecting data and techniques used in analysis. Data was collected using administered questionnaires and interviews. Data was analysed using IBM SPSS Version 25 for descriptive and inferential statistics. The results from the analysis revealed that externally, attacker-victim remoteness, presence of skilled and knowledgeable hackers and fake offers on the internet to share security credentials contribute to information security vulnerabilities in public organizations. The findings unveiled that internally, employees action derived for personal financial gains, ease to execute and available internet tools, disgruntled employees launching retaliatory attacks to sabotage systems and weak information infrastructure systems contribute to information security vulnerabilities in public organizations. Moreover, study findings revealed user awareness training on cyber security issues, carrying out cyber risk assessment on its critical assets and cyber security or information security audits as well as establishing cyber security policy will address the issue information security vulnerabilities in public organizations. The study recommends that same study should be conducted in other institutions and in other countries for comparison and generalization of findings.

LIST OF ABBREVIATIONS AND ACRONYMS

ICT	Information and Communication Technology
IS	Information System
IT	Information Technology
SPSS	Statistical Package for Social Science
TAEC	Tanzania Energy Commission
TEMDO	Tanzania Engineering and Manufacturing Design Organisation

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER ONE

INTRODUCTION

1.1 Introduction

This chapter highlights the main reasons for the study. It also gives the background to the research problems, statement of the problem, research objectives, research questions, and significance of the study. In addition to that, the chapter covers Scope of the study as well as the organization of the study.

1.2 Background to the Study

Information security is basically the process of ensuring the safety of information from known and unknown threats. The International Telecommunication Union states that cyber security is the collective application of strategies, security measures, plans, threats administration tactics, engagements, training, paramount practices, assurance and expertise that can be used to guard the information system, organization and related assets (International Telecommunication Union, 2016). Information security could also refer to the security of internet, computer networks, electronic systems and other devices (Olayemi, 2014) from the cyber-attacks.

Access of an organization information system could have far reaching moments especially in the current time of information edge strategy. An organization can lose its competitive advantage which could lead to its destruction, loss of privacy data leading to law suits and processes, and also loss of trusts by the entity’s stakeholders (Gaudin, 2017). Governments, commercial organizations and individuals around the world have invested heavily in Information and Communications Technologies (ICT), implying the systems’ security is of utmost importance. To achieve this, they deploy technical security measures, and develop security policies that specify the correct behaviour of employees, consumers and citizens. A secure e-government information system guarantees performance of the system and not only enhances reliability, confidence and belief, but also meets the security standards. A secure and reliable information system is recognized as a basis of enhancing confidence of e-government systems (Herath & Rao, 2019).

Availability of government services through e-government besides offering convince to legitimate stakeholders, has also opened critical databases and infrastructure to the risk of attacks (Tassabehji et al. 2017). Infiltration of e-government systems could have an impact on e-government users' systems' confidence and adoption (Ebrahim & Irani, 2018).

Operations in the public entities are different from the private entities operations hence the two necessitates different methods (Moon, 2011). Recently there has been an increase of the public offices engaging and offering services to their users through the ICT infrastructure. The public entities are bound to open deliberations of their strategies, executive and legislative arms deliberations in their funds appropriations leading to political influence, provision of products for public good rather than economic viability and have to be geographically distributed over the administration region irrespective of the economic sense. This implies management of public entities have to align to their specific processes and the respective security models (Wimmer and von Bredow, 2011). Due to the nature of e-government requirement of openness, distribution and availability, e-government systems are a concern for privacy and security issues (Norris and Moon, 2015).

The main justification of e-government systems is to offer public services conveniently and continuously over open and distributed networks. Security reliability of information connected over distributed networks offering convenience to stakeholders is vital not only in the private sector but also in the public sector, however for the public division there is different emphasis (Alfawaz, 2018). An effective information system including e-government systems incorporates personnel, infrastructure, processes and technologies (Alfawaz, 2018). This implies success of e-government systems is a factor of population social features of the country it is being implemented.

Public entities are also subject to review by internal auditors who advise the management on the risk exposer and recommend correction measurers preferably prior to external audit review. While the external audit responsibilities do include the responsibility to assess security as part of certain engagements, the final financial statements audits do not usually include the responsibility to assess cyber security. However, the internal audit IT audit function frequently includes the responsibility to assess cyber security, thus internal auditors are a reliable source of cyber security in public entities (Alfawaz, 2018).

Recently multiple public institutions have been targets of information insecurity; government organizations were victim of cyber-attacks in Tanzania in last years as per the report by Eva (2019). This paper investigated factors that contribute information security in Tanzanian public entities.

1.3 Statement of the Problem

ICT and particularly e-government for developing countries and related cyber security in developing countries is generally under-represented in the open literature; there are very few published empirical studies directly addressing the issue. According to Serianu (2015), the public sector (government and related parastatals) were ranked first on risk levels in information security. Cyber-attacks in government ministries in 2018 caused panic across the country since the intruders had penetrated websites expected to have state secrets, and sensitive security and financial information (Misiko, 2019). Previous researchers have shown inter-relationship between e-government, organization administration and security issues (Dhillon and Torkzadeh, 2016; Heeks, 2013; Siponen and Oinas-Kukkonen, 2017; Von Solms, 2019). Researchers have mainly concentrated on quantitative technical issues to address information systems' security (Siponen and Oinas-Kukkonen, 2017). However objective analysis of information systems' security indicates non-technical issues are essential as technical issues in protecting sensitive information (Dhillon and Torkzadeh, 2016; Siponen and Oinas-Kukkonen, 2017). Previous studies have mainly been undertaken in the developed countries context, implying there is limited open literature relating to dynamics such as environment, population awareness, social culture for developing countries and how the aspects relate to standard approaches towards information system administration. This study expound further to incorporate the external and internal factors that contribute information security in the public organizations.

1.4 Research Objectives

1.4.1 General objective

Generally, this study sought to investigate factors that contribute information security vulnerabilities in public organizations: A case of TEMDO and TAEC - Arusha.

1.4.2 Specific Objectives

i. To establish the external organizational factors that may contribute to information security vulnerabilities in public organizations
ii. To determine internal organizational factors that may contribute to information security vulnerabilities in public organizations

1.5 Research Question

i. What are the external organizational factors that are contributing to the information security vulnerabilities in public organizations?
ii. What are the internal organizational factors that are contribute to information security vulnerabilities in public organizations?

1.6 Scope of the Study

The issue of information security management had beenwidely studied with different approaches and from different perspectives. The study focused on the factors that contribute information security vulnerabilities in TEMDO and TAEC - Arusha. Specifically, the study established the external organizational factors that may contribute to information security vulnerabilities in public organizations and determined internal organizational factors that contribute to information security vulnerabilities in public organizations.

1.7 Limitation of the Study

Despite of the scope the study, the researcher faced the following obstacles.

i. Some of the information was confidential and contributed to some degree of confidentiality being used by the researcher.
i. Financial constraints whereby the researcher faces insufficient funding to conduct the research.
ii. Negligence and some of the respondents as in most researches are busy

1.8 Significance of the Study

The findings of this study will add value to the current body of knowledge to the policy makers, government of Tanzania and security professionals, and researchers and academicians as explained below:

i. The information generated in the course of this study would be important to policy makers since it would guide them when formulating policies and strategies that contribute individual internet end users. This study provides information security professionals with relevant information that would be used to determine how to deal with cyber security threats.

ii. The study would also contribute to information security research as it looks into deficiencies identified from the model analysis and provides improvement strategies against malicious insiders and outsiders. The insight would be useful to individuals employed in critical infrastructure areas as well as security agencies charged with protecting critical assets to assist them build or improve defences against insider and outsider cyber threats.

iii. The information to be generated in the course of study would also enrich the body of knowledge on information security attacks in the country and the Public Service.

iv. To future researchers and academicians, the study would be important in the suggestion of areas requiring further research to build on the topic information security in public entities in Tanzania. In addition, the findings of this study would be important source of reference for future scholars and researchers.

1.9 Organization of the Study

This study is arranged into five chapters. Chapter one introduces the topic to the readers by showing the background of the study and statement of the problem giving a focus of the study. The Objectives of the study indicated. Scope of the study, its significance and organization of the study was also explained. Chapter two present the review of the related literature, where all the concepts that are important to the study was presented. Chapter three described how the study was carried out; showing the methodology of the study in terms of its design and approach, the population and its sample size, types of data and the way data was collected and analyzed. The purpose of this chapter was to present, discuss and argue for the choices made in designing the research framework of this study. Chapter four presents, analyzes and discusses the findings of the study. The analysis and presentation were done in accordance to the specific objectives of the study. The discussion was conducted by comparing the findings with the results of other related studies carried elsewhere. Chapter five summarized the findings of the study, gives the conclusion and recommendation. This chapter also, suggest some other areas to be considered for further researches.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter presents the literature review of the study on the factors that contribute information security vulnerabilities in public entities. It consists of the theoretical literature review, empirical literature review, and research gap. Theoretical literature review provides scientific definitions of the major concepts describing the phenomenon being studied while empirical literature review describes what has been done to solve or address the illogical or contradicting relationship in the phenomenon.

2.2 Theoretical Literature Review

2.2.1. Explanatory Model of Cyber-Attacks Drawn from Rational Choice Theory

A new influence model for evaluating cyber security is presented that deals with security attacks and implementation of security measures from an attacker's perspective (Mandelcorn et al. 2013). The underlying hypothesis of this model is that criminological theory of rational choice is relevant to cybercrime and thereby aids in the understanding its basic motivation. The model includes the roles of consequences, moral beliefs such as shame and embarrassment together with formal sanctions in deterring cybercrime, as well as role of defence posture to limit the opportunity to attack and increase the likelihood that an attacker will be detected and exposed (Manadhata 2007). Few attempts have been made to understand cybercrime in the context of typical crime because of its uniqueness, e.g. attacker-victim remoteness, ease to execute and available internet tools. In developing the model, information from studies in classical crime was related to cybercrime allowing for analysis of past cyber-attacks, and subsequently preventing future cyber-attacks, or mitigating their effects. The influence model's applicability in this study demonstrated by applying it to external and internal organizational factors that contribute to information security vulnerabilities in organizations. The model is also useful in qualitatively explaining "best practices" in protecting information assets and in suggesting measures to address information security vulnerabilities in organizations. This model was used to establish the external and internal organizational factors that may contribute to information security vulnerabilities in public organizations.

2.3 Empirical Literature Review

Wechuli (2014) evaluated cyber security assessment framework in government Ministries in Kenya. The evaluation was on the limiting factors affecting the framework thus exploring on strategy and baseline assessment and prioritization (inventory of assets based of their importance in organizations infrastructure). This research is fairly related to this research as it evaluated the public service though it evaluated the cyber security strategy. This research will evaluate the cyber security in public service with additional factors especially in human and leadership who are the implementers of the framework and still have behavior management incorporated in their administration.

Wekundah (2015) did a study on the effects of cyber-crime on e-commerce for SMEs in Kenya. The study found out that most SMEs do not put emphasis or assign enough resources on cybercrime attack; they also lack expertise and experiences in handling cyber-attack crimes. This study was done in the business sector and its findings may not be applicable in the government ministries.

Nyawanga (2015) studied the meeting the challenge of cyber threats in emerging electronic transaction technologies in Kenyan banking sector. The study found out that the cyber-crime rate has increased in the past 12 months with most 80 percent of attacks originating from China and Kenya itself. The study also found out that cyber-crime is mostly perpetrated by one of the bank staff knowingly or unknowing. Raising concerns for the need for cyber training for most if not all the banking staff. This study was done in the banking sector and its findings may not be applicable in the government ministries in Kenya.

Ibikunle and Eweniyi (2013) did a study on challenges and solution to information security issues in Nigeria. The study recognizes objectives of information security to include: addressing ICT systems and networks vulnerabilities; development and nurturing an information security culture by institutions and individuals; deriving an effective collaboration in information security between private and public organizations even beyond political bounders; keeping in-touch with new developments in cyber-crime and their effective solutions; and ensuring systems availability, confidentiality, integrity and authenticity.

Deshpande and Sambhe (2014) conducted a review of information security by looking at the strategy to security challenges. It identified latest issues on information security in India as including: cyber terrorism; use of internet in cyber terrorism, threat to ICT infrastructure, and information security management. The findings indicate that many users value personal computers on security matters while ignoring security for mobile phones yet attacks can be perpetrated using the phones and the consequences would be as severe just like attacks through personal computers. Personal firewalls can protect individual devices from attacks launched through the "air connection" or from the internet.

Deore and Waghmare (2016) carried out a literature review on information security automation for controlling distributed data. Most of the government and private organizations are trying to protect our data and information from cyber terrorist or hackers. Information security plays important role in information system as well as data sharing. For the protection of important information and data most of the software was developed by many organization using different techniques. Statistics indicate that data sharing was also challenge for government as private organization. Most of the information was hacked at the time of sharing personal or government or official information. Different techniques were developed and used by scientist for the protection of information from attacker.

Alfawaz (2018) on research on security of e-government systems in developing countries and identified key factors that impact on e-government security as top management support, staff and management security awareness, information system security infrastructure, security culture, management style, management change and security and privacy regulations. This paper is a key precursor of this study as is undertaken in the context of the public sector though not specific to Tanzania.

Kyobe (2018) in research on Information Security challenges and their implications for emerging e-government structures in some African Countries denotes that information security is a major limitation caused not only by technological developments as normally perceived in literature, but also by political, cultural, legal and moral behaviours of the society. Further observation in the above paper notes, while the security challenges faced in e-government may not differ from those in the private sector, they are more complex and sensitive because e-government operations involve many citizens and are bound to various legal frameworks and requirements.

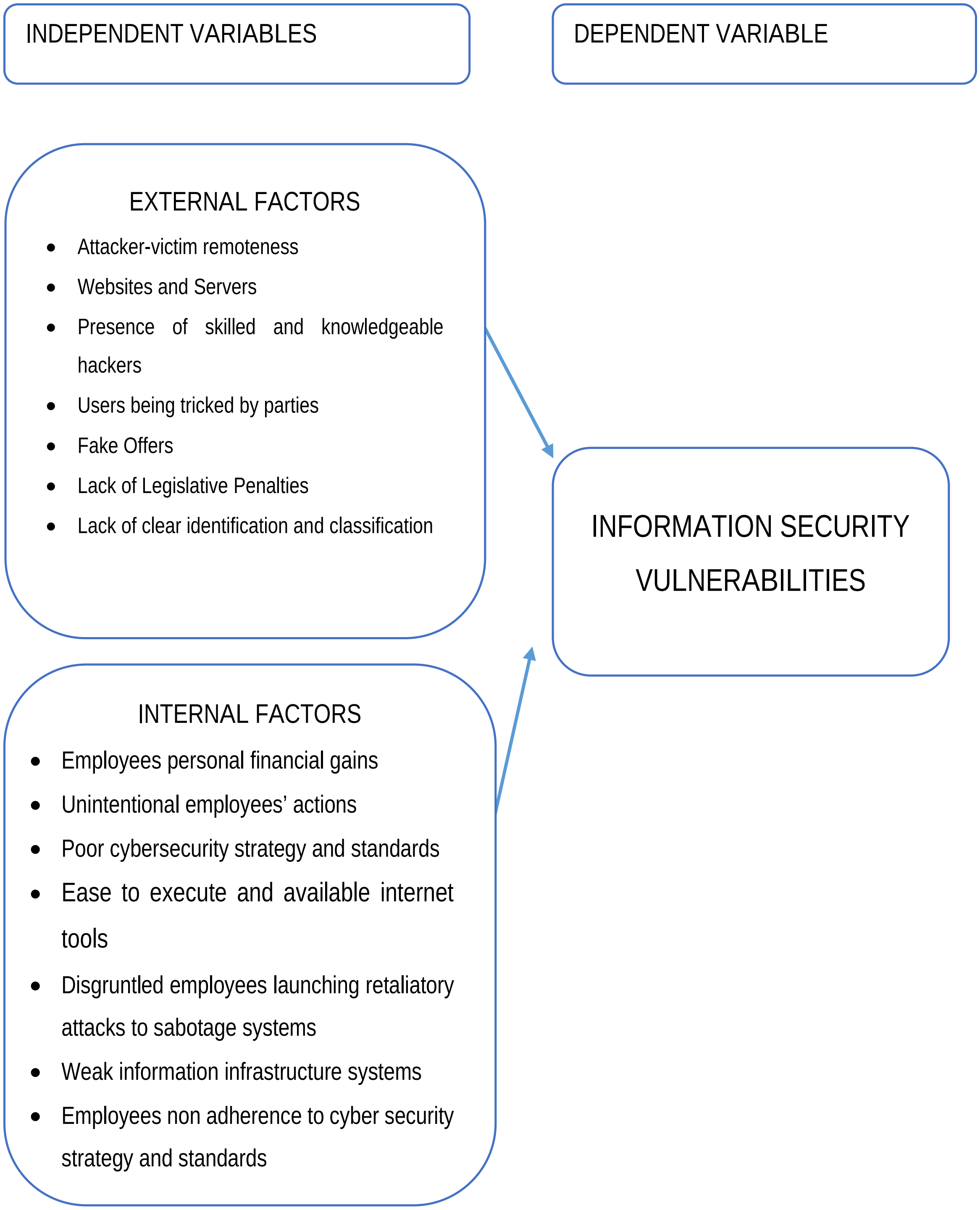
2.4 Research Gap

Based on the above empirical literature, it is evident that a good number of researches similar to this study have been conducted in different places, with recommendations and suggested solutions. However, there was no study that specifically searched for the the factors that contribute information security vulnerabilities in public organization. Therefore, data that collected from this study, the conclusion and recommendations sought to cover the gap.

2.5 Conceptual Framework

Conceptual framework of this study explains relationship between independent variables and dependent variable. Independent variables in this study are internal factors and external factors. Dependent variable of this study is information security vulnerabilities.

Figure 2.1: Conceptual Framework


INDEPENDENT VARIABLES
DEPENDENT VARIABLE
EXTERNAL FACTORS
• Attacker-victim remoteness
• Websites and Servers
• Presence of skilled and knowledgeable hackers
• Users being tricked by parties
• Fake Offers
• Lack of Legislative Penalties
• Lack of clear identification and classification
INFORMATION SECURITY VULNERABILITIES
INTERNAL FACTORS
• Employees personal financial gains
• Unintentional employees' actions
• Poor cybersecurity strategy and standards
• Ease to execute and available internet tools
• Disgruntled employees launching retaliatory attacks to sabotage systems
• Weak information infrastructure systems
• Employees non adherence to cyber security strategy and standards

Source: Researcher (2020)

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This study aims at investigating the factors that contribute information security vulnerabilities in public entities. This chapter specifically presents the methodology that was used to conduct this study. It covers the research design, the target population, sampling design, data collection procedures, the method of data analysis, reliability and validity and ethical considerations while conducting the research

3.2 Research Design

This study was undertaken through the utilization of a descriptive study design. The descriptive study design was adopted because of the way that it permits examination of the relations of variables under study. Also, the reason validates why this study embrace a descriptive research design is because it permits more noteworthy adaptability in terms of time, cash and in addition maintaining a strategic distance from the hardship of chasing for respondents more than once to deliver high response rate (Reeves & Hedberg, 2003).

3.3 Area of the Study

Data was collected at the selected organizations in Arusha. These organizations are; TEMDO and TAEC. Staff in these organization were able to describe in detail the current situation and give recommendations on the factors that contribute information security vulnerabilities in public organizations. This was expressed objectively in the form of words, phrases or text; as in data provided in documents. Further the study area was chosen due to familiarity and convenience of a researcher to access information.

3.4 Research Population, sampling techniques and Sample Size

3.4.1 Population

According to Saul (2003) research population is also known as a well-defined collection of individuals or objects known to have similar characteristics. All individuals or objects within a certain population usually have a common, binding characteristic or trait. Under this research, the target population were managers and employees from the selected entities as summarized in Table 3.1.

3.5 Sampling techniques

The researcher used census sampling design in selected sample of this study. According to Crossman (2018) census is often construed as the opposite of a sample as its intent is to count everyone in a population rather than a fraction. The researcher used this sampling technique so that to get accurate information as it included all important respondents who are aware of the the factors that contribute information security vulnerabilities.

3.5.1 Sample Size

The study consisted of employees from TEMDO and TAEC. This research used the sample size of 37 staff as outlined in the table below;

Table 3.1: Sample size

Respondents	TEMDO	TAEC	TOTAL
IT Managers	1	1	2
ICT officers	3	6	8
Users (PMU, HR, Accounts)	15	25	40
TOTAL			50

Source: Researcher, 2020

3.6 Data Collection Methods

Singh, (2006) asserted that the data collection is the accumulation of specific evidence that will enable the researcher to properly analyse the results. The main purpose of data collection is to verify the research questions. The study aimed at collecting information from managers and employees at the selected entities in Arusha on the the factors that contribute information security vulnerabilities through questionnaires and semi-structured interview instrument. The researcher used both primary and secondary data where by primary data was gathered through administering questionnaires and semi-structured interviews. Secondary data was obtained through document reviews.

i. Questionnaire

According to Kothari (2004) questionnaire implies a technique of data collection where there is a direct contact between the researcher and respondents. A self-administered questionnaire was developed for this study to facilitate primary data collection. The questionnaire was used to collect primary data on measurements of independent and dependent variables.

ii. Interviews

The researcher follows a rigid procedure and seeks answers to a set of pre-conceived questions through personal interviews (Kothari, 2004). This method of collecting data is usually carried out in a structured way where output depends upon the ability of the interviewer to a large extent. The researcher used this method to collect data from managers and employees at the selected entities.

3.7 Data Analysis

Collected data was summarized, classified, presented and analysed using Inferential statistics with a readily available technology to research such as Statistical Package for Social Scientists (SPSS). The rationale behind using these packages rested in their extensive analytical capacity and easiest in administering data. This required both quantitative and qualitative data. In explaining some research findings, descriptive statistics was employed also. The results to be obtained from data analysis was presented in tables and figures.

3.8 Validity and Reliability of Data

The concepts of reliability and validity are core issues in determining the quality of a study. In order for a study to provide sufficiently sound, consistent, and relevant evidence, the information provided must be both reliable and valid (Joppe, 2000). Therefore, both reliability and validity in this study were ensured and achieved through checking inaccuracies or missing information at various points in the collection, maintenance, processing, and reporting of data, proper processing and reporting of data, usage of proper sampling procedures in order to obtain a representative sample, careful selection of standardized data collection instruments (questionnaire and interview).

3.8.1 Reliability

Reliability requires the use of standardized information collection instruments and survey procedures that are designed to enhance consistency.

3.8.2 Validity

Validity is the extent to which the survey information is relevant to the conclusion being drawn and is sufficiently accurate and complete to support the conclusion, Validity determines whether the research truly measures that which it was intended to measure or how truthful the research results are (Joppe, 2000).

3.9 Ethical Considerations

During the research, the researcher exercised confidentiality; anonymity and privacy so as to safeguard the interviewees and other respondents all together. The researcher avoided deception in the process of conducting the research and was honest about the aims and goals and procedures of the study. The respondents were assured that the information they provide were carefully analysed and the report produced mainly as a dissertation for submission to Institute of Accountancy Arusha for requirement in partial fulfilment for the award of Masters of Information Technology Management.

CHAPTER FOUR

PRESENTATION AND DISCUSSION OF FINDINGS

4.1 Introduction

This chapter presents the results of the analysis and findings of the study. Data was collected using questionnaires and interviews as the data collection instruments and summarized by use of descriptive statistics which involved the use of frequency tables.

4.2 Response Rate

Respondents of this study received 50 questionnaires, and all 50 questionnaires were returned and used for analysis representing 100% response. This is a reliable response rate for analysis as Mugenda and Mugenda (2003) showed that 50% of response rate is sufficient for analysis and presentation of the data, 60% is reliable and 70% of response rate and over is excellent. This response rate was considered adequate and representative to allow generalization of the findings.

4.3 Presentation of Findings

This section present findings as obtained in the field. The data collected was analysed using measures of central tendency and the results presented in tables

4.3.1. Demographic Information

Demographic information of the respondents were analysed and presented in the table below;

Table 4.1: Demographic Information

Details		Frequency	Percent
Gender	Male	35	70
	Female	15	30
Age of the Respondents	18-24 Years	1	2
	25-34 Years	20	40
	35-44 Years	19	38
	45 Years and above	10	20
Education Level	Certificate	3	6
	Diploma	15	30
	Bachelor Degree	25	50
	Postgraduate	7	14
Service Duration	Below 2 Years	5	10
	2-5 Years	16	32
	6-10 Years	25	50
	Above 10 Years	4	8
6%	Yes	38	76
	No	10	20
	Not Sure	2	4
Organization use information systems in course of service delivery	Yes	48	96
	No	2	4

Source: Field Data 2020

The analysis revealed that most of the respondents were men. Specifically, the data showed that 70% of the respondents were men while 30% were female. This shows that the researcher was not biased on the gender when data was collected, even though the males were responding than female. The table above most of the respondents 40% were aged from 25 - 34 years' old while the rest of the respondents under the same group 38% were aged from 35-44 years old. These respondents were distributed in this range as it separate youth from adults. Analysis showed that, the majority of the respondents were Degree holders. Also, the table above showed that majority of the respondents were experienced enough to share their opinions concerning the problem under the study as most of the have been working for 6 – 10 years (50%). On the issue of cyber-attack, majority of the 76% agreed that their organization have been a victim of cyber-attack. This may be attributed to the reason that the in one way or another these organizations information systems in course of service delivery as indicated by 96% of total population.

4.3.2 External Factors

This section sought to establish the external organizational factors that may contribute to information security vulnerabilities in public organizations. The following are findings presented in the table below 4.2;

Table 4.2: External Factors

Statement		SD	D	N	A	SA
Attacker-victim remoteness	F	0	0	11	23	16
	(%)	0	0	22	46	32
Presence of skilled and knowledgeable hackers	F	0	0	0	26	24
	(%)	0	0	0	52	48
An attack that resulted in websites and servers unavailable to legitimate users	F	0	8	10	30	2
	(%)	0	16	20	60	4
Users being tricked by parties external to the organization to give out their security information for example passwords	F	0	0	16	17	17
	(%)	0	0	32	34	34
Fake offers on the internet to share security credentials	F	0	1	20	20	9
	(%)	0	2	40	40	18
Lack of legislative penalties for cyber-attacks implication	F	0	6	13	14	17
	(%)	0	12	26	28	34
Lack of clear identification and classification of ICT assets and exposure involved	F	12	0	9	29	0
	(%)	24	0	18	58	0

SD=strongly disagree D= Disagree N=Neutral A=Agree SA=Strongly Agree

Source: Field Data 2020

From the table above, majority of the respondents (46%) agreed and (32%) strongly agreed that Attacker-victim remoteness contribute to information security vulnerabilities in public organizations while 22% were neutral. 52% and 48% of the respondents agreed and agreed respectively that presence of skilled and knowledgeable hackers contribute to information security vulnerabilities in public organizations. 64%t of the respondents agreed that an attack that resulted in websites and servers unavailable to legitimate users contribute to information security vulnerabilities in public organizations though 20% of the respondents were neutral and 16% disagreed In this study (68%) of the respondents agreed that users being tricked by parties external to the organization to give out their security information for example passwords contribute to information security vulnerabilities in public organizations while 32% of the respondents were neutral. 58% of the respondents agreed that fake offers on the internet to share security credentials passwords contribute to information security vulnerabilities in public organizations, 2% disagreed and 48% were neutral. Majority of respondents (32%) agreed that lack of legislative penalties for cyber-attacks implication contribute to information security vulnerabilities in public organizations however 26% were neutral and 12% disagreed. 58% of the respondents agreed that lack of clear identification and classification of ICT assets and exposure involved contribute to information security vulnerabilities in public organizations yet 24% of the respondents disagreed and 18% were neutral. Users of ICT assets have to well alerted about the risks and threats involved with the assets they are using in their day to day operations.

4.3.3 Internal Factors

This section sought to determine internal organizational factors that may contribute to information security vulnerabilities in public organizations. The following are findings presented in the table below 4.3;

Table 4.3: Internal Factors

Statement		SD	D	N	A	SA
Employees action derived for personal financial gains	F	0	0	18	28	4
	(%)	0	0	36	56	8
Lack of support for acquisition and development of cyber security human skills (personnel)	F	0	2	10	24	14
	(%)	0	4	20	48	28
Ease to execute and available internet tools	F	0	3	7	25	15
	(%)	0	6	14	50	30
Disgruntled employees launching retaliatory attacks to sabotage systems	F	9	3	14	24	0
	(%)	18	6	28	48	0
Unintentional employees' actions but leading to systems attack ministry cyber security policy and standards deficiency	F	17	2	5	26	0
	(%)	34	4	10	52	0
Poor implementation and adherence of cyber security strategy and standards by involved management	F	4	16	10	20	0
	(%)	8	32	20	40	0
Weak information infrastructure systems	F	0	5	12	30	3
	(%)	0	10	24	60	6
Employees non adherence to cyber security strategy and standards	F	8	7	4	31	0
	(%)	16	14	8	62	0

SD=strongly disagree D= Disagree N=Neutral A=Agree SA=Strongly Agree

Source: Field Data 2020

From the table above, majority of the respondents (64%) agreed that employees action derived for personal financial gains contribute to information security vulnerabilities in public organizations while 36% were neutral. Findings unveiled that majority of the respondents (76%) agreed that lack of support for acquisition and development of cyber security human skills contribute to information security vulnerabilities in public organizations while 20% were neutral and only 4% were neutral.

80%t of the respondents agreed ease to execute and available internet tools contribute to information security vulnerabilities in public organizations though 14% of the respondents were neutral and 6% disagreed

In this study (48%) of the respondents agreed that disgruntled employees launching retaliatory attacks to sabotage systems contribute to information security vulnerabilities in public organizations, 18% strongly disagreed 6% disagreed and 23% of the respondents were neutral. 52% of the respondents agreed that unintentional employees' actions but leading to systems attack ministry cyber security policy and standards deficiency contribute to information security vulnerabilities in public organizations, 4% disagreed, 34% strongly disagreed and 10% were neutral. Majority of respondents (40%) agreed that poor implementation and adherence of cyber security strategy and standards by involved management however 20% were neutral, 32% disagreed and 8% strongly disagreed. 66% of the respondents agreed that weak information infrastructure systems contribute to information security vulnerabilities in public organizations yet 24% of the respondents were neutral and 10% disagreed. Majority of respondents (62%) agreed that employees non adherence to cyber security strategy and standards contribute to information security vulnerabilities in public organizations, 8% were neutral, 14 disagreed and 16% strongly disagreed. To the large extent non adherence to cyber security measures and cautions by employees lead the company into insecurity fumble.

4.4 Test of Reliability and Validity

4.4.1 Reliability

Reliability of questionnaire was tested using Cronbach's alpha. The results in table 4.5 indicate that the reliability of data instruments was acceptable since Cronbach alpha was 0.701 for all items as indicated by Hair et al., (2003) that when Cronbach' alpha is greater than 0.6 is still acceptable.

Table 4.5 Reliability Statistics

Reliability Statistics		
Variables	Cronbach Alpha	Internal Consistency
All Items	0.701	Acceptable
External Factors	0.762	Acceptable
Internal Factors	0.704	Acceptable

Source: Field data 2020

4.4.2 Validity

The Kaiser-Meyer-Olkin (KMO) and Bartlett test was used to test validity. According to Cerny (1977), if the test is 0.0 to 0.45 the internal adequacy in explanatory factor is unacceptable. When it is 0.50 to 0.59 is poor; 0.60 to 0.79 is acceptable; when 0.8 to 0.89 is good and 0.9 to 0.99 is excellent.

The result of the test indicated that KMO had a value of .606, which is acceptable. On the other hand, Bartlett test in this study yield p-value =0.00 which signify that the variables are correlated highly enough to provide a reasonable basis for factor analysis as suggested by (Hooper, 2012) that the value for Bartlett test should be a significant value of less than .05 as describe below in KMO and Bartlett test table 4.6.

Table 4.6: KMO and Bartlett's Test

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.606
Bartlett's Test of Sphericity	Approx. Chi-Square	1271.047
	Df	780
	Sig.	.000

Source: Field Data 2020

4.5 Analysis of Inferential Statistics

4.5.1 Correlation Analysis

Pearson correlation coefficient was used to determine the strength and the direction of the relationship between the dependent variable and the independent variable. The analysis using Pearson's product moment correlation was based on the assumption that the data is normally distributed and also because the variables are continuous.

Table 4.7: Correlations

Correlations				
		External Factors	Internal Factors	Information Security Vulnerabilities
External Factors	Pearson Correlation	1	.834**	.790**
	Sig. (2-tailed)		.000	.000
	N	50	50	50
Internal Factors	Pearson Correlation	.834**	1	.791**
	Sig. (2-tailed)	.000		.000
	N	50	50	50
Information Security Vulnerabilities	Pearson Correlation	.790**	.791**	1
	Sig. (2-tailed)	.000	.000	
	N	50	50	50
**. Correlation is significant at the 0.01 level (2-tailed).				

Source: Field Data 2020

The study showed that there was a strong correlation between the Independent variables and audit quality. Internal Factors gave the highest magnitude of 0.791 while A External Factors gave a slightly lower magnitude of 0.790. This means that External Factors and Internal Factors with Information Security Vulnerabilities.

4.5.2 Regression Analysis

In addition, the researcher conducted a multiple regression analysis so as to test joint effect of Internal Factors, External Factors on Information Security Vulnerabilities.

Table 4.8: Model Summary

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate

1	.826[a]	.682	.668	.66866
a. Predictors: (Constant), Internal Factors, External Factors				

Source: Field Data 2020

The adjusted R^2 was found to be 0.682 inferring that variations on Information Security Vulnerabilities which are explained by Internal Factors, External Factors were 68.2%.

Table 4.9: ANOVA results

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	45.066	2	22.533	50.398	.000[b]
	Residual	21.014	47	.447		
	Total	66.080	49			
a. Dependent Variable: Information Security Vulnerabilities						
b. Predictors: (Constant), Internal Factors, External Factors						

Source: Field Data 2020

In predicting the effects of Internal Factors, External Factors on Information Security Vulnerabilities, the regression model test was found to be significant since p-value was less than 0.005 and The calculated F (50.398) was larger than the critical value of F=2.7426.

Table 4.10: Regression Coefficients

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	8.468	1.007		8.407	.000
	External Factors	.240	.083	.429	2.884	.006
	Internal Factors	.129	.044	.433	2.908	.006
a. Dependent Variable: Information Security Vulnerabilities						

Source: Field Data 2020

The established model for the study was:

$Y= 8.468+0.241X1 + 0.129X2 +\alpha$

The results reveal that quality audit will be 8.468 if all other factors are held constant. The study results also show that an increase in External Factors will lead to a 0.240 increase the Information Security Vulnerabilities if all other factors are held constant. Again as shown by r=0.129, the study revealed that increase in Internal Factors would lead to an increase in the Information Security Vulnerabilities if all other factors are held constant. Regression analysis shows how dependent variable is influenced with independent variables.

4.6 Interview Analysis

Five ICT officers participated in the interviews. The interview data was transcribed then coded into themes according to research objectives. Regarding personal information, their responses to research objectives are as follows:

4.6.1 External Organizational Factors

The objective was to assess external organizational factors that are contributing to the information security vulnerabilities in public organizations. During the interview, the respondents asserted the two major external factors which are;

i. Internet and Advance tools

Respondents indicated that availability of technological tools (such as computers, software and hardware) and internet across the globe enhances convenience for legitimate users but it also avails critical assets and infrastructure to threat of cyber-attack by illegitimate users.

ii. Activities of the illegitimate users

Interviewees stated that Information security vulnerabilities in public organizations are motivated by various interests which usually vary but not exclusive for different groups. These groups are hacking exploitation; serious and organized crime; ideological and political extremism; and state sponsored cyber-aggression.

4.6.2 Internal Organizational Factors

On the internal organizational factors that are contribute to information security vulnerabilities in public organizations. On the interview, respondents stated that;

i. Employees retaliating their "unfair" treatment in the organization contribute much to information security vulnerabilities in public organizations
ii. Organization insiders exploiting the company's assets for their self-interested gains contribute much to information security vulnerabilities in public organizations
iii. Also, unintended cyber attackers' insiders who are primarily not the attackers but who unsuspectingly facilitate outside attacks contribute to information security vulnerabilities in public organizations

4.6.3 Measures to address information security vulnerabilities

Respondents gave their views and opinions as to measures that should be done to address information security vulnerabilities in public organizations. Respondents stated that to address information security vulnerabilities, public organizations they should do the following:

i. Use strong passwords

Users should use strong passwords, password that is difficult to guess. Respondents insisted that password must contain a combination of capital and lower-case letters, numbers and symbols, password of at least eight characters long and the password must be changed regularly.

ii. Access control

Respondents proclaimed that, Public organizations should make sure that their systems can only be accessed to the users that are authorized for. The access control includes physical access control to premises and computers network, restriction of access to unauthorized users, limit access to data or services through application controls and limit sending and receiving of certain types of email attachments.

iii. Firewall

Interviewees asserted that firewalls are effectively gatekeepers between their computer and the internet, and one of the major barriers to prevent the spread of cyber threats such as viruses and malware. Public organizations should make sure that their firewall devices work properly for the sake of server security.

iv. Security Software

Respondents stated, Public organizations should use security software to address information security vulnerabilities. Security software, such as anti-spyware, anti-malware and anti-virus programs, will help detect and remove malicious code if it slips into their network.

v. Update programs and systems regularly

Either they averred that Public organizations should regularly updated their programs and systems. The reason behind is that updates contain vital security upgrades that help protect them against known bugs and vulnerabilities.

vi. Raise awareness

Lastly, important thing above all, the respondents stated that Public organizations should do and trying hard to make sure that users especially employees understand their role, policies and procedures concerning information security and cyber threats henceforth provide them with regular cyber security awareness and training. This is because employees have a responsibility to help keep their organizations safe and secured.

4.7 Discussion of Findings

Infiltration of an organization information system could have far reaching consequences especially in the current era of information edge strategy. An organization can lose its competitive advantage which could lead to its extinction, loss of privacy data leading to law suits and litigations, and also loss of trusts by the entity's stakeholders. Study findings unveiled that, attacker-victim remoteness, presence of skilled and knowledgeable hackers and an attack that resulted in websites and servers unavailable to legitimate users contribute to information security vulnerabilities in public organizations. Availability of internet across the globe with sophisticated software and hardware enhances convenience for legitimate users but it also avails critical assets and infrastructure to threat of information vulnerabilities by illegitimate users. These findings are in line with Khalid (2016) that information security vulnerabilities are highly attributed with the current advancement of technological tools which can easily facilitate information infiltration and presence of smart Information technology specialists.

Even with firewalls, antivirus solutions, and cyber security awareness training for your employees, cybercriminals still manage to exploit any vulnerabilities they can find. This could be because they exploit attack vectors that are known to your organization (but remain unaddressed for some reason) or because they've discovered vulnerabilities that are not yet known to you (Crane, 2019) Also findings uncovered that users being tricked by parties external to the organization to give out their security information, fake offers on the internet to share security credentials passwords contribute to information security vulnerabilities in public organizations. This is because whether with intent or without malice, people are the biggest threats to cyber security. These vulnerabilities come from employees, vendors, or anyone else who has access to network or IT-related systems.

Findings indicated that lack of legislative penalties for cyber-attacks implication and lack of clear identification and classification of ICT assets and exposure involved contribute to information security vulnerabilities in public organizations. These findings collaborate Pelgrin (2014) absence of the ICT assets guidelines and legislative penalties influences information security vulnerabilities in organizations.

Kundy (2019) asserted that cyber-attacks occasionally are instigated by insiders who can broadly be classified in three categories; i) organization employees retaliating their "unfair" treatment in the organization; ii) organization insiders exploiting the company's assets for their self-interested gains; and iii) unintended cyber attacker's insiders who are primarily not the attackers but who unsuspectingly facilitate outside attacks. Her findings support findings of this study where by the researcher findings' designated that employees action derived for personal financial gains, lack of support for acquisition and development of cyber security human, ease to execute and available internet tools and disgruntled employees launching retaliatory attacks to sabotage systems contribute to information security vulnerabilities in public organizations,

Researcher discovered that unintentional employees' actions contribute to information security vulnerabilities in public organizations. These findings collaborates the findings of Andress (2018) and the finds of Nyawanga (2016) on cyber threats in Kenyan banking sector which showed that cybercrime is mostly perpetrated by one of the entity's staff knowingly or unknowingly.

Even with firewalls, antivirus solutions, and cyber security awareness training for your employees, cybercriminals still manage to exploit any vulnerabilities they can find. This could be because they exploit attack vectors that are known to your organization (but remain unaddressed for some reason) or because they've discovered vulnerabilities and flaws that are not yet known to you (Crane, 2019). Findings of this indicated that poor implementation and adherence of cyber security strategy and weak information infrastructure systems contribute to information security vulnerabilities in public organizations. This is consistent with Alfawaz (2015) findings who identifies keys factors that impact on information security as top management support, staff and management security awareness, weak information system security infrastructure, security culture, management style, management change and security and privacy regulations. Infrastructure has always been considered a legitimate target. Study findings found that employees non adherence to cyber security strategy and standards contribute to information security vulnerabilities in public organizations. There is a need to educate employees on using ICT infrastructures, assets and exposures because unknown cyber threat can be accidentally transfer from a portable device from home directly into organization's system.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

A considerable number of items are covered by this study on analysis of factors that contribute information security vulnerabilities in public organizations. This chapter bears the summary of findings, implications, limitations of the study; conclusion and finally the need for further research.

5.2 Summary of Findings

The first objective was to establish the external organizational factors that may contribute to information security vulnerabilities in public organizations. The findings indicated that attacker-victim remoteness contribute to information security vulnerabilities in public organizations and 48% of the respondents agreed and agreed respectively that presence of skilled and knowledgeable hackers contribute to information security vulnerabilities in public organizations. Majority of the respondents (64%) of the respondents agreed that an attack that resulted in websites and servers unavailable to legitimate users contribute to information security vulnerabilities in public organizations. In this study (68%) of the respondents agreed that users being tricked by parties external to the organization to give out their security information for example passwords contribute to information security vulnerabilities in public organizations while 58% of the respondents agreed that fake offers on the internet to share security credentials passwords contribute to information security vulnerabilities in public organizations. Majority of respondents (32%) agreed that lack of legislative penalties for cyber-attacks implication contribute to information security vulnerabilities in public organizations however 58% of the respondents agreed that lack of clear identification and classification of ICT assets and exposure involved contribute to information security vulnerabilities in public organizations.

The second objective was to determine internal organizational factors that may contribute to information security vulnerabilities in public organizations. Findings indicated that employees action derived for personal financial gains contribute to information security vulnerabilities in public organizations. This was indicated by 64% of the entire population. Findings unveiled that majority of the respondents (76%) agreed that lack of support for acquisition and development of cyber security human skills contribute to information security vulnerabilities in public organizations while 80%t of the respondents agreed ease to execute and available internet tools and disgruntled employees launching retaliatory attacks to sabotage systems contribute to information security vulnerabilities in public organizations. 52% of the respondents agreed that unintentional employees' actions but leading to systems attack ministry cyber security policy and standards deficiency contribute to information security vulnerabilities in public organizations. Majority of respondents agreed that poor implementation and adherence of cyber security strategy and standards by involved management as well as weak information infrastructure systems contribute to information security vulnerabilities in public organizations. Majority of respondents (62%) agreed that employees non adherence to cyber security strategy and standards contribute to information security vulnerabilities in public organizations.

5.3 Conclusion

This study concludes that factors that contribute information security vulnerabilities in public organizations are principally divided in to external factors and internal factors. The major external factors that contribute to information security vulnerabilities in public organizations were identified as; attacker-victim remoteness, presence of skilled and knowledgeable hackers, fake offers on the internet to share security credentials and lack of legislative penalties for cyber-attacks implication. The internal organizational factors that contribute to information security vulnerabilities in public organizations were identified as; employees action derived for personal financial gains, lack of support for acquisition and development of cyber security human skills, ease to execute and available internet tools and unintentional employees' actions but leading to systems attack ministry cyber security policy and standards deficiency as well as poor implementation and adherence of cyber security strategy and standards by involved management. To address information security vulnerabilities in public organizations, this study postulated that users to get proper training on cyber security issues while organization continuous monitoring of inbound network traffic load on firewalls and system resources and carrying cyber risk assessment hence establish cyber security policy which will ensure that users abide to the technological rules of the organizations.

5.3 Critical Evaluation of the Study

Regardless of the challenges encountered by the researcher, the researcher managed to deliver this report in time. In this research, externa factors and internal factors contributing to information security vulnerabilities in public organizations was revealed. I would like to carry a study on the organizational and human factors affecting computer and information security if I had to do the same task.

5.4 Recommendation for Future Research

Given the time constraint at hand for the researcher, the researcher therefore recommends further detailed research into the review of cyber security by looking at the strategy to security challenges in public institution - Tanzania. Also, same study should be conducted in other institutions and in other countries for comparison and generalization of findings.

REFERENCE

Alfawaz (2015) 'E-government security in developing countries: a managerial conceptual framework', paper presented to International Research Society for Public Management Conference, Queensland University of Technology, Brisbane,

Alfawaz, S. (2018) 'E-government security in developing countries: a managerial conceptual framework', paper presented to International Research Society for Public Management Conference, Queensland University of Technology, Brisbane, 26-28 March 2088

Andress (2018) Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness,MIS Quarterly34(3), 523-548

Crane, (2019) he privacy privilege: Law enforcement, technology and the constitution. Journal of Technology Law and Policy 7 (2) 123-94.

Crossman, Ashley(2018),understanding purposive sampling: an overview of the method and its applications. Retrivedfrommhttps://www.thoughtco.com/purposive-sampling-3026727 on October, 9th 2019.

Deore and Waghmare (2016) "Implementing enterprise security: A case study", Computers & Security (7:6), 2003, pp. 99-114, 2016

Deshpande and Sambhe (2014) "Organisational factors to the effectiveness of implementing information security management" Industrial Management & Data Systems (106:3) 2006, pp 345-361.

Dhillon, G., &Torkzadeh, G. (2016). Value-focused Assessment of Information Systems Security in Organizations, Information Systems Journal16(3), 293- 314.

Ebrahim & Irani, (2018) Cybercrime, cybersecurity and the future of the internet

Gaudin, H. (2017) "Computer security policy: important issues", Computers & Security (l7:6), pp. 1988, pp. 559-562,.

Geer Dan (2016) An Integrative Study of Information Systems Security Effectiveness, International Journal of Information Management (23), 139-154

H Herath, T., & Rao, H. R. (2019). Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organizations.European Journal of Information Systems18(2), 106-125.

Hamilton, T. (2002) Encryption and Evolving Technologies: Tools of Organized Crime and Terrorism, Working Group on Organized Crime, National Strategy Information C Washington.

Heeks, U. (2013) Study of Latest Emerging Trends on Cyber Security and its Challenges to Society, International Journal of Scientific & Engineering Research, 3(6), 124-132

Hussein and Khalid (2016) SCADA Insecurity-Stuxnet put the Spotlight on Critical Infrastructure Protection but Will Efforts to Improve it come too late?Information Security Magazine, 13(1), 38-44.

Ibikunle and Eweniyi (2013) Social media and national security threats: a case study of Kenya (Doctoral dissertation, University of Nairobi)

International Telecommunication Union, (2016) Understanding Cybercrime: A Guide for Developing Country.

Joppe, M. (2000). The research process. Examining the validity structure of qualitative and quantitative research, 118(3), 282-292.

Khalid (2016) “Investigating the Factors Inhibiting SMEs From Recognizing and Measuring Losses From Cyber Crime in South Africa” The Electronic Journal Information Systems Evaluation Volume 14 Issue 2 2011, (pp167-178),

Kothari, C. R. (2004). Research Methodology: Methods and Techniques. New Age International

Kundy S.,W. (2018). Toward a criminal law for cyberspace, Distributed Security. Boston University Journal of Science & Technology Law 10 (2).

Kyobe, M. (2018). Evaluating Information Security within SMEs engaged in Ecommerce in South Africa. Institute for Small Business & Entrepreneurship, 5- 7.

Moon F. (2011) How Anonymous and other Hackitivists are waging war on Kenya. The Washington Post.

Norris and Moon (2015) Effects of Cybercrime on State Security: Types, Impact and Mitigations with the Fiber Optic Deployment in Kenya, Journal of Information Assurance & Cyber security.

Nyawanga (2016) "Exploring organizational culture forinformation security management," Industrial Management & DataSystems, vol. 107, no. 3, pp. 438- 458.

Nyawanga J. O. (2015). Meeting the challenge of cyber threats in emerging electronic transaction technologies in in Kenyan banking sector (Doctoral dissertation, University of Nairobi).

Olayemi, (2014) Investigating the Effectiveness of IS Security Countermeasures Towards Cyber Attacker Deterrence. 2012 45th Hawaii International Conference on System Scienc (pp. 1-10). Hawaii: Nova Southeastern University

Pelgrin (2014) Organized crime? How cyberspace may affect the structure of criminal relationships. North Carolina Law & Technology 4 (1)

Pelgrin (2014) Theoretical Trace and Framework of Overall Innovation Management. Chinese Journal of Management, 2, 002.

Reeves & Hedberg, (2003) Monitoring the Effectiveness of Security. Institut Supérieur de Gestion de Tunis publication (pp. 327 -336). Tunis: Institut Supérieur de Gestion de Tunis.

Saul, S. (2003) Organizational Security Culture: Extending the End-User Perspective. Computers & Security, 26 (1), 56-62

Schuessler, S. (2009) An Approach To Enhance ICTInfrastructures' Security Through Legal, Regulatory Influence. In J. E. HS Venter (Ed.), ISSA 2005 New Knowledge Today Conference. Sandton, South Africa..

Serianu Consultants in Cyber Security (2015); available at ahttp://www.usiu.ac.ke/oncampus/news/296-serianu-usiu-africa-pkf-consulting-launch-kenya-cybersecurity-report-2015

Singh, Y. K. (2006). Fundamental of Research Methodology and Statistics. New Delhi: New Age International Publisher

Siponen and Oinas-Kukkonen, (2017) Enterprises Must Prepare to Combat Cyber Espionage. Clearwater, Florida: hreatTrack Security, Inc

Tassabehji et al. (2017) A Security Audit Framework to Manage Information System Security. ICGS(3), 9-18.

Von Solms, (2019) Cyber Security: Challenges for Society- Literature Review, Journal of Computer Engineering, 12(2), 67-75

Wechuli A. (2014) on Cyber Security Assessment Framework: Case of government Ministries in Kenya; International Journal of Technology in Computer Science and Engineering, 1(3).

Wekundah, R. N. (2015). The effects of cyber-crime on e-commerce; a model for SMEs in Kenya (Doctoral dissertation, University of Nairobi).

Wimmer and von Bredow, (2011) Security challenges as a factor affecting the security of manet: attacks, and security solutions. International Journal of Network Security & Its Applications (IJNSA) Vol.7, No.3,

APPENDICES

APPENDIX I: DATA COLLECTION LETTER

I am Nelson Misheto, a student from Institute of Accountancy Arusha (IAA). I am conducting research on the factors that contribute information security vulnerabilities in public organizations and therefore the purpose of this questionnaire is to capture information that will reflect the study topic. I kindly ask you to assist me in my study by completing the questionnaire. I assure you that your information will be kept confidential.

APPENDIX II: QUESTIONNAIRE

PART ONE: DEMOGRAPHIC INFORMATION

Gender	Male □ Female □
Age	18-24 Years □ 25-34 Years □ 35-44 Years □ 45 Years and above □
Highest Level of Education	Certificate □ Diploma □ Bachelor Degree □ Postgraduate □
Duration at the Organization	Below 2 Years □ 2-5 Years □ 6-10 Years □ Above 10 Years □
Has the Organization been a victim of cyber attack	Yes □ No □ Not Sure □
Does the organization use information systems in course of service delivery	Yes □ No □

PART TWO: ACADEMIC RESEARCH QUESTIONS (Tick the appropriate answer)

SECTION A: EXTERNAL ORGANIZATIONAL FACTORS

The following part seeks to stablish the external organizational factors that may contribute to information security vulnerabilities in public organizations

EXTERNAL ORGANIZATIONAL FACTORS	Options				
	1	2	3	4	5
Attacker-victim remoteness					
Presence of skilled and knowledgeable hackers					
An attack that resulted in websites and servers unavailable to legitimate users					
Users being tricked by parties external to the organization to give out their security information for example passwords					
Fake offers on the internet to share security credentials					
Lack of legislative penalties for cyber-attacks implication					
Lack of clear identification and classification of ICT assets and exposure involved					

1=strongly disagree 2= Disagree 3=Neutral 4=Agree 5=strongly agree

SECTION B: INTERNAL ORGANIZATIONAL FACTORS

The following part seeks to determine internal organizational factors that may contribute to information security vulnerabilities in public organizations

INTERNAL ORGANIZATIONAL FACTORS	Options				
	1	2	3	4	5
Employees action derived for personal financial gains					
Lack of support for acquisition and development of Cyber security human skills (personnel)					
Ease to execute and available internet tools					
Disgruntled employees launching retaliatory attacks to sabotage systems					
Unintentional employees' actions but leading to systems attack Ministry cyber security policy and standards deficiency					
Poor implementation and adherence of cyber security strategy and standards by involved management					
Weak information infrastructure systems					
Employees non adherence to cyber security strategy and standards					

1=strongly disagree 2= Disagree 3=Neutral 4=Agree 5=strongly agree

SECTION C: MEASURES

The following part seeks to recommend measures to address information security vulnerabilities in public organizations

MEASURES	Options				
	1	2	3	4	5
User awareness training on cyber security issues					
Continuous monitoring of inbound network traffic load on firewalls and system resources (CPUs)					
Segmentation of internal and external networks for critical systems					
Carry out cyber risk assessment on its critical assets					
Carry out cyber security or information security audits					

Constantly scanning and patching for software vulnerabilities					
Maintain staff values and attitudes that align with organizational mission and ethic					
Cyber security policy					

1=strongly disagree 2= Disagree 3=Neutral 4=Agree 5=strongly agree

Thank for your cooperation!

INTERVIEW GUIDE

Head of Departments and IT specialists from each Organization will be interviewed to obtain more detailed information concerning the factors that contribute information security vulnerabilities in public organizations.

1. What are the external organizational factors that are contributing to the information security vulnerabilities in public organizations?
2. What are the internal organizational factors that are contribute to information security vulnerabilities in public organizations?
3. What measures should be done to address information security vulnerabilities in public organizations?

Thank you very much for your time and for responding to my questions!

RESEARCH BUDGET

1. Budget estimated

My organization will cover the estimated research budget costs.

Table 1: Budget estimated

Activity	Input description	Unit of measure	Cost @ unit	Number of Units	Amount to student
Objective 1:• To examine how cybersecurity is perceived by banks employees.					
To collect data from employees TEMDO and TAEC	Per diem for student	Day	20,000	10	200,000
	Transport	Days	5000	10	50,000
	Stationary	ream of paper	8,000	5	40,000
		printing toner	35,000	1	35,000
		folders	1,000	2	2,000
		A bag	20,000	1	20,000
	Labour charge	Day	5,000	10	50,000
Subtotal					397,000
Objective 2: To determine the challenges facing banks in Tanzania in creating cybersecurity awareness among their employees.					
	Per diem	Day	20,000	10	200,000
	Transport	Days	5000	10	50,000
		printing toner	35,000	1	35,000
	Labour charge	Day	5,000	10	50,000
Subtotal					335,000
Objective 3: To explore strategies adopted by banks in Tanzania to create awareness of their employees on cybersecurity.					
	Per diem	Day	20,000	10	200,000
	Transport	Days	5000	10	50,000
		printing toner	35,000	1	35,000
	Labour charge	Day	5,000	10	50,000
Subtotal					335,000
Total					1,067,000

Source; Researcher (2020)

SCHEDULE OF ACTIVITIES

Research schedule is a plan for carrying out a process or procedure, giving lists of intended events and times. The thesis schedule table is described below:

Table 2: Gantt chart

Activities	Dates					
	Jan	Feb	Mar	Apr	May	Jul
Formulating and refining Research Problem	■					
Reviewing Literatures	■	■				
Draft of Research Proposal Writing to Supervisor		■	■			
Research Proposal Defence			■			
To Submit Proposal and Data collection letter processing			■			
Data collection				■		
Data Processing/Management					■	
Data analysis					■	
Draft Report Writing to Supervisor					■	
Final Report Defence						■
Final Report Corrections						■
Binding and Final Submission						■

Source; Researcher (2020)

NELSON MISHETO REPORT.docx

ORIGINALITY REPORT

10%	8%	2%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	scholor.mzumbe.ac.tz Internet Source	4%
2	daad.wv.tu.harburb.de Internet Source	5%
3	link.springer.com Internet Source	1%

Exclude quotes	On	Exclude matches	< 2%
Exclude bibliography	On		