THE PRACTICE OF INFORMATION SECURITY: AN ANALYSIS OF GOVERNMENT EMPLOYEES IN TANZANIA USING THE HEALTH BELIEF MODEL (HBM)

DANIEL NTABAGI KOLOSENI

DOCTOR OF PHILOSOPHY

FACULTYOF BUSINESS AND FINANCE
UNIVERSITI TUNKU ABDUL RAHMAN
NOVEMBER 2017

THE PRACTICE OF INFORMATION SECURITY:

AN ANALYSIS OF GOVERNMENT EMPLOYEES IN TANZANIA

USING THE HEALTH BELIEF MODEL (HBM)

By

DANIEL NTABAGI KOLOSENI

A Thesis submitted to the Faculty of Business and Finance,

Universiti Tunku Abdul Rahman,

in partial fulfilment of the requirements for the degree of Doctor of Philosophy

November 2017

DEDICATION

To the most peculiar people in my life, my wife Neema Rolland Mushi, my parents Celina Koloseni and the late Michael Koloseni, my late Sister Asteria, my children Abigail, Abraham, Hannah, Sara and Henry whose loving, caring and sacrifices they have made, manifest on every page of this work.

ABSTRACT

THE PRACTICE OF INFORMATION SECURITY: AN ANALYSIS OF GOVERNMENT EMPLOYEES IN TANZANIA USING THE HEALTH BELIEF MODEL (HBM)

Daniel Ntabagi Koloseni

E-Government information systems need to be protected to ensure secure delivery of information services to the citizens. Lack of information security awareness, poor perceptions with regard to the susceptibility and severity of information security attacks, benefits and barriers of practising security behaviours and poor information security habits among Tanzania government employees, jeopardise the success of the e-government initiatives in Tanzania. To address the above issues, this study extends and uses the Health Belief Model (HBM) as a foundational research model of the study.

To measure hypothetical relationships between the constructs of the research model, the study employed the structural equation modelling (SEM) technique. *Process* macro was used to test the mediation relationships. Data were collected using questionnaires from the government employees tasked to operate the e-government information systems.

The study found that perceived severity, perceived susceptibility, perceived barriers, cues to action and information security habits, were key determinants

of intention to practice information security behaviours. In addition, intention to practice information security was the key determinant of the actual practice of information security. Mediation analysis results indicate that perceived severity construct mediates the relationships between the level of education of the government employees and intention to practice information security behaviours.

In order to motivate government employees to practice the acceptable information behaviours, policy and decision makers should invest more efforts in increasing the intention of government employees to practice information security and its respective determinants. To achieve this, information security training, education programs, information security awareness campaigns, rewards, sanctions, dialogue between employees and security experts and cues should be used.

This study contributes to the body of knowledge in the following ways: 1) extending the model by adding two variables; information security habits and actual practice of information security behaviours, 2) examining the mediation effects of individual perceptions on the relationships between education level and intention to practice information security behaviours and 3) addressing the knowledge gap on paucity of studies which measures the influence of information security habits on the intention to practice information security behaviours.

ACKNOWLEDGEMENT

First and foremost, I would like to thank Almighty God for taking me through this journey. God, you listened and answered my prayers whenever I sought your face, definitely, all of this could have not been possible without you.

Second, I would like to thank my supervisors, Dr Chong Yee Lee and Dr Gan Ming Lee for their constructive advices and guidance throughout my study. Special thanks go to Dr Chong Yee Lee for her tireless efforts for consistently responding to my emails on time and sharpened my research methodology knowledge. From her, I have learnt a lot of value for my future endeavours. My thanks also go to Dr Gengeshwari a/p Krishnapillai for her valuable advice and comments, particularly, during data analysis. I would like also to extend my thanks to internal examiner Dr Mobashar Rehman, and two external examiners Prof Timothy Mwololo Waema and Associate Prof George Oreku for their constructive comments.

Third, I would like to thank my employer, The Institute of Finance Management (IFM) for the sponsorship and permission to pursue this study. Fourth, many thanks to fellow doctoral students for the moral support in different phases of my PhD study. In particular, I would like to thank Jumanne Basesa, Edmund Kimaro, Herman Mandari, Julius Macha and Zacharia Elias.

There are many other people who contributed to this research work in one way

or another and I wish, it would have been possible to list them all. All those I met during the research process, relatives, friends and colleagues, I appreciate your contributions and I candidly thank you all.

Last but not least, I am eternally grateful to Neema Rolland Mushi my lovely wife and soul mate, who was courageous enough to let me go abroad and leave her with the family to take care of and who graciously, stood by me through the ups and downs of my studies. I cannot thank her enough. Also, I would like to thank my Mother Celina Koloseni, brother Dr David Koloseni and his wife Dr Pendo Kivyiro, my young brother Dunstan and my sisters Lydia and Eva for their prayers, unconditional love and constant support.

APPROVAL SHEET

This thesis entitled "**THE PRACTICE OF INFORMATION SECURITY: AN ANALYSIS OF GOVERNMENT EMPLOYEES IN TANZANIA USING THE HEALTH BELIEF MODEL (HBM)**" was prepared by DANIEL NTABAGI KOLOSENI and submitted as partial fulfillment of the requirements for the degree of Doctor of Philosophy at Universiti Tunku Abdul Rahman.

Approved by:

_____

(Dr. CHONG YEE LEE) Date: ……
Supervisor
Department of Marketing
Faculty of Business and Finance
Universiti Tunku Abdul Rahman

_____

(Dr. GAN MING LEE) Date: ……
Co-supervisor
Department of Computer and Communication Technology
Faculty of Information and Communication Technology
Universiti Tunku Abdul Rahman

SUBMISSION SHEET

FACULTY OF BUSINESS AND FINANCE

UNIVERSITI TUNKU ABDUL RAHMAN

Date: _____

SUBMISSION OF THESIS

It is hereby certified that **DANIEL NTABAGI KOLOSENI** (ID No: **15ABD01269)** has completed this thesis entitled "THE PRACTICE OF INFORMATION SECURITY: AN ANALYSIS OF GOVERNMENT EMPLOYEES IN TANZANIA USING THE HEALTH BELIEF MODEL (HBM)" under the supervision of Dr Chong Yee Lee (Main Supervisor) from the Department of Marketing, Faculty of Business and Finance, and Dr Gan Ming Lee (Co-Supervisor) from the Department of Computer and Communication Technology, Faculty of Information Communication Technology.

I understand that the University will upload softcopy of my thesis in pdf format into UTAR Institutional Repository, which may be made accessible to UTAR community and public.

Yours truly,

_____

DANIEL NTABAGI KOLOSENI

DECLARATION

I **DANIEL NTABAGI KOLOSENI** hereby declare that the thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at UTAR or any other institution.

_____

DANIEL NTABAGI KOLOSENI

Date : _____

TABLE OF CONTENTS

Page

DEDICATION **II**

ABSTRACT **III**

ACKNOWLEDGEMENT **V**

APPROVAL SHEET **VII**

SUBMISSION SHEET **VIII**

DECLARATION **IX**

LIST OF TABLES **XIV**

LIST OF FIGURES **XVI**

LIST OF ABBREVIATIONS **XVII**

CHAPTER

1.0 INTRODUCTION **1**

1.1 Introduction 1

1.2 Background of the Study 1

1.3 Problem Areas 4

1.3.1 Problem Statement 7

1.4 Research Questions 8

1.5 Research Objectives 9

1.6 Significance of the Study 10

1.6.1 For Policy Makers 10

1.6.2 For Academic 11

1.7 Scope and Delimitation of the Study 13

1.8 Organisation of the Thesis 14

2.0 LITERATURE REVIEW **16**

2.1 Introduction 16
2.2 Overview Theoretical Frameworks 16
2.2.1 General Deterrence Theory (GDT) 17
2.2.2 The Health Belief Model (HBM) 19
2.2.3 Protection Motivation Theory (PMT) 23
2.2.4 Theories of Reasoned Actions (TRA) and Planned Behaviours (TPB) 26
2.2.5 Technology Threat Avoidance Theory (TTAT) 28
2.2.6 Justification for Using the HBM 30
2.2.7 Summary of the Relevant Theoretical Frameworks in Information Security Behaviour 32
2.3 Overview of Research Models that used HBM Theory 34
2.3.1 Relevant Past Study's Measurement Items 38
2.4 Overview of the Past Studies' Research Methodology 42
2.5 Overview of Relevant Past Studies' Data Analysis 47
2.6 Summary of Literature Review 50
2.7 The Proposed Research Framework 51

3.0 RESEARCH METHODOLOGY 58

3.1 Introduction 58
3.2 Development of Current Research's Hypotheses 58
3.3 Research Design and Philosophy 69
3.3.1 Rationale for the Choice of the Research Paradigm 71
3.4 Sampling Design 72
3.4.1 Definition of Target Population 72
3.4.2 Survey Location 73
3.4.3 Sampling Technique and Procedures 74
3.4.4 Sample Size 76
3.5 Instrument and Data Collection Procedures 77
3.5.1 Development of the Questionnaire 77
3.5.2 Pre-test Procedures and Results 83
3.5.3 Pilot study Procedures and Results 86
3.5.4 Data Collection Period for Main Survey 91
3.5.5 Representativeness of Data to the Population 94
3.5.6 Data Analysis Techniques, Tools, and Requirements 95

3.5.7 Missing Values Analysis 96
3.5.8 Data Normality Assessment and Outliers 96
3.5.9 Multicollinearity Tests 99
3.5.10 Measurement and Structural Model Validation 99
3.5.11 Hypotheses Testing, Direct and Indirect Effects 103
3.6 Summary of the Current Study' Research Methodology 105

4.0 FINDINGS AND DISCUSSION 106

4.1 Introduction 106
4.2 Respondent's Descriptive Information and Response rate 106
4.3 Data Screening and Normality Assessment 108
4.3.1 Missing Value Analysis Results 108
4.3.2 Univariate and Multivariate Normality 109
4.3.3 Multivariate Outliers 110
4.3.4 Correlation Estimates and Multicollinearity Results 111
4.4 Confirmatory Factor Analysis Results 112
4.5 Validity, Reliability and Unidimensionality 116
4.6 Common Method Variance Results 121
4.7 Structural Model Results 123
4.8 Hypotheses Testing Results 129
4.8.1 Direct Effects on Intention to Practice Information Security 129
4.8.2 Mediation Effects on Intention to Practice Information Security 136
4.9 Squared Multiple Correlations (R^2) 141
4.10 Summary 142

5.0 CONCLUSION 144

5.1 Introduction 144
5.2 Accomplishment of Research Objectives 144
5.3 Theoretical Implications 148
5.4 Policy Implications 150
5.5 Limitations 158
5.6 Direction for Future Research 159

REFERENCES **161**

APPENDICES **191**

Appendix A: List of e- Services 191
Appendix B: Consent forms, Ethical approval and Questionnaires 192
Appendix B1: A Sample Consent Form 192
Appendix B2: Ethical Approval Letter 195
Appendix B3: Pre- Test Questionnaire for Refinement 196
Appendix B4: Pre- Test Questionnaire for Rating 204
Appendix B5: Pilot Study Questionnaire 213
Appendix B6: Main Study Questionnaire 219
Appendix C: Outliers Assessment Results 224
Appendix D: Cook's Distance and Leverage Test Results 226
Appendix E: Correlations Estimates for Constructs 230
Appendix F: Adjusted Measurement Model: Item PSEV 2 Deleted 231
Appendix G: Adjusted Measurement Model: Item CUE 1 Deleted 232
Appendix H: Adjusted Measurement Model: Item HAB4 Deleted 233
Appendix I: Adjusted Measurement Model: Item SE3 Deleted 234
Appendix J: CMV Results –Harman's Single Factor Test 235
Appendix K: Constructs Studied in the Past Studies 236

BIODATA OF THE STUDENT **238**

LIST OF TABLES

Table **Page**

2.1: Weaknesses and Strengths of Relevant Theoretical Frameworks 33
2.2: A Summary of Past Research Models that used HBM 35
2.3: Relevant Constructs and Items used in the Past Studies 39
2.4: Summary of Past Studies Research Methodology 46
2.5: Summary of Relevant Past Studies Data Analysis Techniques 49
2.6: Definitions of the Constructs of the Study 56
3.1: Relationships between Objectives and Hypotheses 69
3.2: Distribution of Government Institutions in Tanzania (MDAs) 73
3.3: Distributions of Respondents for MDAs 75
3.4: The Measurements Items for Pilot Study Questionnaire 78
3.5: Results of Pre-test 85
3.6: Respondents Distribution for Pilot Study 87
3.7: Demographic Information of Respondents for the Pilot Study 87
3.8: Results of Pilot Items Reliability Analysis 88
3.9: Results of Factor Analysis 90
3.10:Model fit and Cut- off Values 102
4.1: Respondent's Demographic information for the Main Study 107
4.2: Missing data cases and MCAR test results 108
4.3: Univariate Normality Assessment Results 109
4.4: Variance Inflation Factor Results 112
4.5: Model Fit Results for Initial Measurement Model 113
4.6: Item Factor Loadings 115
4.7: Model fit results for the final measurement model 116
4.8: Inter-item Correlations CR and AVE Score for each Construct 117
4.9: Standardised Item Factor Loadings 117
4.10: Construct Mean scores 120
4.11: Harman's Single Factor Test Results 121
4.12 :Common Latent Factor Test Results 122
4.13: Model Fit Results for Initial Structural Model 124

4.14: Modification Indices Scores 127
4.15: Model Fit Results for Final Structural Model 127
5.1: Summary of Major Findings and Policy Implications 157

LIST OF FIGURES

Figure	Page
2.1: General Deterrence Theory	18
2.2: Theoretical Framework of the Original Health Belief Model	20
2.3: Theoretical Framework of Modified Health Belief Model	22
2.4: Theoretical Framework of Protection Motivation Theory	25
2.5: Theoretical Framework of Theory of Reasoned Action	27
2.6: Theoretical Framework of Theory of Planned Behaviour	28
2.7: Technology Threat Avoidance Theory	30
2.8: Current study's Research Framework	55
3.1: Current study's Research Model	67
4.1: Initial Measurement Model	114
4.2: Final Measurement Model	119
4.3: Initial Structural Model	126
4.4: Final Structural Model	128
5.1: Final Research Framework with Standard Estimates	147

LIST OF ABBREVIATIONS

ANOVA	Analysis of Variance
AVE	Average Value Extracted
CFA	Confirmatory Factor Analysis
CMV	Common Method Variance
e-GMM	Electronic Government Maturity Model
GDT	General Deterrence Theory
GNMC	Government Network Management Centre
HBM	Health Belief Model
ICT	Information Communication Technology
IS	Information Systems
MDA	Ministries, Departments and Agencies
MMR	Moderated Multiple Regressions
NICTBB	National ICT Backbone
PMT	Protection Motivation Theory
REPOA	Research on Poverty Alleviation
SEM	Structural Equation Modelling
SMS	Short Message Service
TCRA	Tanzania Communications Regulatory Authority
TPB	Theory of Planned Behaviour
TRA	Theory of Reasoned Action
TTAT	Technology Threat Avoidance Theory
TZ-CERT	Tanzania Computer Emergence Response Team
UN	United Nations
URT	United Republic of Tanzania
USP	Unified Security Practices

CHAPTER 1

INTRODUCTION

1.1 Introduction

This chapter provides the background statement of the research problem, research questions and objectives of the study. Also, it states the significance of the study to academics, policy and decision makers, scope and the limitations of the study. Lastly, it provides the description and arrangement of the rest of the chapters in this thesis.

1.2 Background of the Study

In recent years, the government of Tanzania has successfully established a substantial number of e-government initiatives, such as the provision of e-mails, online plot allocation, online payment of bills, online tax payments, as well as dissemination of online financial information and reports. The e-Government services have also been incorporated into the education system. For example, students can view their examination results, apply for student loan, register for admission in higher learning institutions and social funds membership by using information communication technology (ICT) gadgets or online system (Sawe, 2007; URT, 2013;URT, 2016) (See appendix A, page number 191 for the list of other e-services offered by the government).

The services provided by e-government information systems are beneficial to the government and citizens in terms of acceleration of work processes, improvement in transparency and accountability, as well as reduction of operation costs. To realise the benefits, government employees were trained to use ICT systems. For example, using emails, operating a computer and its applications and use of e-government systems to generate and disseminate reports. As of the year 2017, more than 13,000 government employees were trained (Domasa, 2017).

Several agencies that relate to the e-government initiatives were established. National ICT Backbone (NICTBB) was set-up in 2009 to ensure a reliable and speedy internet connectivity, by developing a high-speed broadband network which offers end to end user data protection using fibre optic technology. Lately, in 2012, the Computer Emergency Response Team (TZ-CERT) was established to ensure high level of efficiency of networks and information security; develop the culture of practising information security among users; enhance security for the information transacted between e-Government domains; and respond proactively or reactively to incidences related to information security (TCRA, 2012).

To achieve its objectives, currently, TZ-CERT provides the following services to the general public and institutions: (1) issuing of security alerts and warnings mainly through its website and (2) providing a step by step procedures to solve security incidents to affected institutions (TZCERT, 2017). However, the current services provided by TZ-CERT are not sufficient to develop an

information security culture and enhancing acceptable information security behaviours among the users.

In addition, the Government Network Management Centre (GNMC) was established to host the central government ICT node (Sawe, 2007; TCRA, 2012; URT, 2013). The main purpose of government ICT node is to re-distribute secure communications which involve voice and data for government networks. To prosecute cyber-crime acts such as illegal access to information system, interception and interference of data and information, as well as data espionage, cyber security law was enacted in 2015. Generally, keen efforts were taken to address the technical issues related to the e- government information systems such as acquisition of hardware and software, and provision of ICT training to government employees (Oreku & Mtenzi, 2012).

As government employees are the main users of the e-government information systems and responsible for the provision of e-Government services to citizens, it is essential to investigate their information security behaviours. The employees' information security behaviours, in fact, will influence the performance of the e-government information systems. This is because the government employees (i.e. users of information systems) are the weakest link in the information security chain, even in the presence of state-of-the-art security technologies and security policies (Ani, He, & Tiwari, 2017; Böhme & Moore, 2016; Mitnick & Simon, 2011; Schneier, 2011). In fact, their behavioural actions, either intentional or unintentional, may cause the security vulnerabilities to e-Government information systems (Sebescen & Vitak,

2017). For instance, sharing systems password with other users and connecting office computers with a personal modem or wireless router or person storage devices could threaten the security of e-Government information systems (Agudelo, Bosua, Ahmad, & Maynard, 2016; Alagbe, 2016; Stanton, Stam, Mastrangelo, & Jolton, 2005a). For example, hackers could circumvent organisational security controls, open paths for information security attacks if personal modem or wireless router is used, and the use of personal storage devices could transfer malicious and deleterious software programmes into the e-government systems.

1.3 Problem Areas

Despite of ICT training provided to government employees and the establishment of TZ-CERT which oversees information security issues, Tanzanian e-Government systems are exposed to dangerous information security risks and threats (Dewa & Zlotnikova, 2014; Elisa, 2017; Karokola, 2010; Lupilya, 2016; Lupilya & Jung, 2015).Therefore, it would be worthwhile to study other possible reasons for such information security risks and threats.

Literature suggests that information security threats to e-government information systems could be due to : First, poor individual perceptions with regard to susceptibility and severity of security threats, benefits of practising information security, and the existence of various barriers to exercise information security behaviours (Dewa & Zlotnikova, 2014; Pahnila, Siponen, & Mahmood, 2007; TCRA, 2012; Waziri & Yonah, 2014a). Second, lack of

information security awareness and inadequate security skills such as the inability to apply proper security measures in case of security incidents (Dewa & Zlotnikova, 2014; Bakari, Tarimo, Yngstrom, & Magnusson, 2005; Semboja, Silla, & Musuguri, 2017; Shaaban, Conrad, & French, 2012).

Third, inappropriate information security habits such as a norm of sharing login credentials with colleagues, family members, friends and acquaintances to access government ICT system (Shaaban, 2014); and the habit of connecting personal modems to workplace's mobile gadgets for internet accessibility that could pave the path for attackers to hack or misuse the organisation's information systems (Bakari, 2013; Dewa & Zlotnikova, 2014). In summary, employees' information security behaviours could be the strong contributor to security incidents.

Additionally, Tanzania government employees possess different levels of academic qualifications. Different studies asserted that the level of education qualification could directly influence an individual's behaviours such as intention to (1) adopt certain ICT system (Kongaut & Bohlin, 2016), (2) engage in unsafe driving behaviours (Newnam, Mamo, & Tulu, 2014), and (3) self-manage individual's health (Worth & Dhein, 2004). In other words, education level may influence the current respondents' intention to practice information security behaviours.

In connection to that, Strecher and Rosenstock (1997) asserted that the following variables: perceived susceptibility, severity, benefits and barriers

could mediate the relationship between individual's education level on behavioural intention. Although studies on the mediation of the above-mentioned variables have been carried out in health care (NCHS, 1975; Rundall & Wheeler, 1979), studies in information security are limited**.** Henceforth, this question is raised, could perceived susceptibility, severity, benefits and barriers mediate the effects of Tanzanian government employees' education level on their intention to practice information security behaviours?

Although many studies have been carried out to study individual's behavioural intention (Ando, Shima, & Takemura, 2016; Herath et al., 2014; Yang & Lee, 2016), behavioural intention may not always lead to actual practice of the behaviour in question (Hsu & Huang, 2010;Shropshire, Warkentin, & Sharma, 2015) because what an individual intends to do may not be what an individual actually does (Herath, 2013). Therefore, even if Tanzanian government employees could have the intention to practice information security; there is no guarantee that they will eventually perform the actual information security behaviours. Further, since e-government systems are currently used, the need arises to investigate employees' actual information security behaviours when using e-government information systems.

1.3.1 Problem Statement

Tanzania Government employees have poor perceptions with regard to susceptibility and severity of security attacks, also benefits and barriers of practicing information security behaviours (Dewa & Zlotnikova, 2014; Pahnila, Siponen, & Mahmood, 2007; TCRA, 2012; Waziri & Yonah, 2014a). In addition, they lack information security awareness, possess inadequate information security skills (Dewa & Zlotnikova, 2014; Bakari, Tarimo, Yngstrom, & Magnusson, 2005; Semboja, Silla, & Musuguri, 2017; Shaaban, Conrad, & French, 2012) and they exhibit poor information security habits while using government information systems. This situation exposes e-government information systems to security attacks (Shaaban, 2014). To avoid such attacks and in view of the importance of strengthening information security in e-government service delivery, it is important to conduct an in-depth investigation on Tanzanian government employees' information security behaviours.

The practice of information security behaviours among Tanzanian government employees could be categorised into two groups: (1) conscious security behaviours, which refers to behaviours that are performed by a user who is aware of its actions (Safa et al., 2015) such as responding to a potential susceptible security threats that could occur if a user violated information security procedures, responding to cues (such as advices and recommendations) from security experts on how to avoid security attacks and others.

(2) Non-conscious behaviours in which a user perform a behaviour or an action without thinking or with minimal mental efforts such as automatically log off a computer system after using or before leaving an office, regular virus scanning (termed security habit) and others (Qing, 2016; Verplanken, Myrbakk, & Rudi, 2005).

1.4 Research Questions

In addressing the research problems, the following research questions were developed:

1) To what extent do the employees' perceptions of susceptibility, severity, benefits, barriers, self-efficacy, cues and information security habit could directly affect their intention to practice the information security behaviours?

2) Can education level attained by the employees generate the direct effect on intention to practice information security behaviours?

3) Would the employees' perceptions of susceptibility, severity, benefits, and barriers mediate the effect of education level on their intention to practice information security behaviours?

4) Would employees' intention to practice information security eventually affect their actual practice of information security behaviours?

1.5 Research Objectives

In general, this study examines the extent to which government employees' intention to practice information security which could, in turn, lead to their actual information security behaviours.

Specifically, this study intends:

1) To evaluate the direct effect generated by the perceptions of susceptibility, severity, benefits, and barriers, self-efficacy, cues and the practice of security habit on government employees' intention to practice information security behaviours.

2) To examine the direct effect created by the level of employees' education qualification on their intention to practice information security behaviours.

3) To estimate the effects generated by perceived susceptibility, severity, benefits, and barriers in mediating the effect created by education level on government employees' intention to practice information security behaviours.

4) To evaluate the direct effect of intention of employees to practice information security behaviours towards their actual information security practice.

1.6 Significance of the Study

1.6.1 For Policy Makers

This study is useful for policy and decision makers in three different ways. First, the study may help decision and policy makers in determining information security efforts that are crucial for the management of information security within organisations. Besides, information security efforts (training, awareness programs, and information security investments) could be integrated with the e-Government maturity model (e-GMM) for successful implementation of e-Government initiatives.

In fact, each e-GMM level portrays various technical and non-technical information security requirements, which are required in ensuring maturity of e-Government (Hassan & Khalifa, 2016;Karokola, Kowalski, & Yngström, 2011; Waziri & Yonah, 2014a). Technical requirements include security technologies and controls, while non-technical requirements are comprised of the security behaviours exhibited by end users.

Second, the outcomes of this study could help the policy makers to plan and organise various programmes that will be aimed at encouraging government employees to practice information security behaviours. This is supported by Hanus and Wu, (2016), Ng et al., (2009) and Rhodes (2001) such that

developing effective information awareness campaigns, users' information behaviours should be taken into account.

Third, development of information security culture solely relies on the awareness and comprehension of information security behaviours among its users (Alfawaz, Nelson & Mohannak, 2010; Salleh & Janczewski, 2016) Moreover, understanding the behaviours of information security exhibited by individuals can help many organisations to prioritise their efforts towards information security (Alfawaz et al., 2010; Stanton et al., 2005). Accordingly, understanding information security behaviour provides a platform for the development of a better information security culture for effective management of behaviours linked to information security. In addition, several organisations with the task to oversee e-Government initiatives and cultivation of information security cultures, such as e-Government Agency and TZCERT, are among the beneficiaries of this particular study.

1.6.2 For Academic

This study is useful for academics in four different ways. First, to the best of current researchers' understanding, prior researches on information security have yet to extend the HBM model to measure non-conscious behaviours such as information security habits. The addition of an essential variable: information security habit into the HBM may increase the capability of the model to measure future study respondents' conscious and non-conscious behaviours.

Second, the model has also been extended through the inclusion of another variable: information security behaviour that is used to reflect respondents' actual information security behaviour. The original HBM model was limited to measure only the intention to practice a particular behaviour. According to Hsu and Huan (2010), the behavioural intention may not necessary lead to actual behaviour. Therefore, the model's extension could enrich the HBM.

Third, unlike prior studies, such as those carried out by Claar (2011), and Claar and Johnson (2012), this study estimates both the direct and indirect effects of education level on employees' intention to practice information security behaviours. Moreover, to the best of the researcher's knowledge, limited studies have examined the direct and indirect effects of one's education level through the constructs of perceived susceptibility, severity, benefits and barriers upon the intention to practice information security behaviours or in other words, the mediation effects of perceived susceptibility, severity, benefits and barriers on the relationship between education level and intention, as stipulated in the original HBM. In a different stance, the extended model may also contribute to the healthcare field, where the HBM model originated. For instance, the extended model may be tested in the context of healthcare to measure non-conscious health-related behaviours. Moreover, the empirical testing of the extended model may add value to future researchers in the healthcare field.

Fourth, Pahnila et al. (2007) suggested that information security habits could enhance respondents' intention to practice information security. Thus, determining the relationship between information security habits and information security behavioural intention is indeed important. This is because end-users who possess a certain level of security habits may likely to perform acceptable information security practices.

1.7 Scope and Delimitation of the Study

This thesis focuses on the investigation of information security behavioural perceptions of Tanzania government employees' working at the ministries, independent departments, and authorities (MDAs). Information security behaviours encompass a variety of behaviours such as secure behaviours when opening email attachments, compliance with ICT security policies and others. This study investigates safe computing practices when accessing websites since the majority of e-government services are accessed through the web-based systems. Furthermore, only Tanzanian government employees who use the government information systems in their daily activities participated in the study.

Besides, this study uses the HBM as the basic research model to address the above-highlighted research problems concerning security of Tanzania e-government systems. This model has been tested by many past researchers such as (Abraham, Sheeran, Abrams, & Spears, 1996; Brown, DiClemente, & Park, 1992; Claar, 2011; Hingson, Strunin, Berlin, & Heeren, 1990; Ng et al.,

2009) and their findings are supporting the direct effects generated by perceived susceptibility, severity, benefits, barriers, self-efficacy and cues on respondents' intention to practice information security. Further justification for using this model is found in chapter 2.

Various studies have been carried out to investigate conscious behaviours such as (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009; Chan et al., 2005; Claar, 2011; Claar & Johnson, 2012; Dinev, 2008; Hanus & Wu, 2016; Liang & Xue, 2009; Ng et al., 2009; Pahnila et al., 2007; Pahnila, Siponen, & Mahmood, 2007; Safa et al., 2015; Workman et al., 2008), but only a handful have examined the influence of both conscious and non-conscious information security actions on information security behaviours (Vance, Siponen, & Pahnila, 2012; Yoon, Hwang, & Kim, 2012). Vance, Siponen and Pahnila (2012).

Since many studies have shown that both conscious and unconscious behaviours could possibly affect the intention of government employees' to practice information security, this study investigates both conscious and non-conscious behaviours as well.

1.8 Organisation of the Thesis

This thesis is arranged into five main chapters. Chapter one is about the introduction. One of the main purposes of this chapter is to point-out the issues and their relevant problems that have been overlooked by the Tanzanian

government in the context of information security. Thus, this chapter provides research background, research problem, research questions, objectives, and the significance of the study. Also, it defines the scope and delimitations of the study so that the research can be feasibly conducted and be able to create new knowledge to academics and policy makers.

Chapter two involves a thorough review of literature which examines the applicability of relevant theories and models, research methodologies, and data analysis techniques in this study. After studying the different values highlighted by the past researchers, the present researcher tries to resolve the conflicts so that cohesive conceptual frameworks that cover the research model and research methods, can be built.

In chapter three, the research methodology undertaken for this study is defined. In addition, the pilot test results are highlighted. Chapter four presents and discusses the main findings: descriptive and inferential statistical results. On top of confirming the hypotheses, plausible explanations were given to explain why the hypotheses were supported and not supported.

Finally, chapter five highlights the achievement of the research objectives, theoretical and policy implications of the study, limitations of findings of the study, and direction for future research.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter covers the analysis of the relevant literature on information systems (IS) adoption and behaviour theories that explain what drives human beings towards a specific behaviour. Many theories have been used to explain human behaviours in different contexts. Although the literature on behavioural theories covers a variety of theories, this chapter focuses on theories that have been widely used to explain human information security behaviours when using information systems. Specifically, this chapter reviews the following theories: General Deterrence Theory (GDT), Health Belief Model (HBM), Theory of Reasoned Action (TRA), Theory of Planned Behaviour (TPB), Protection Motivation Theory (PMT), and Technology Threat Avoidance Theory (TTAT), and the modifications that had been done on those theories by the past researchers.

2.2 Overview Theoretical Frameworks

This section provides an overview of relevant theories that have been widely used in the past studies to explain human behaviours in different contexts. Also, originality of the theories and modifications that were done by the past

studies are discussed as the step towards selection of the relevant theory for this study.

2.2.1 General Deterrence Theory (GDT)

This theory was initially developed to address criminal related issues. The theory predicts that individuals would be discouraged to perform deviant behaviours if and only if they perceive consequences of their actions could be serious such as facing or going through a lawsuit (Williams & Hawkins, 1986).This theory has three core constructs which are perceived sanctions severity, perceived detection certainty and perceived celerity of sanctions. Ugrin & Pearson (2013) define GDT's constructs as follows: Perceived sanctions severity refers to one's belief that an individual will be punished for participating in a deviant behaviour. They further define perceived deterrence certainty as the probability that an individual will be caught by participating in a deviant behaviour. Whereas, perceived celerity refers to how swift the sanctions could be put into effect. Perceived celerity of sanctions may modify individual's participation in a deviant behaviour when potential punishment is compared against potential benefits). Relationships between GDT constructs are shown in figure 2.1.

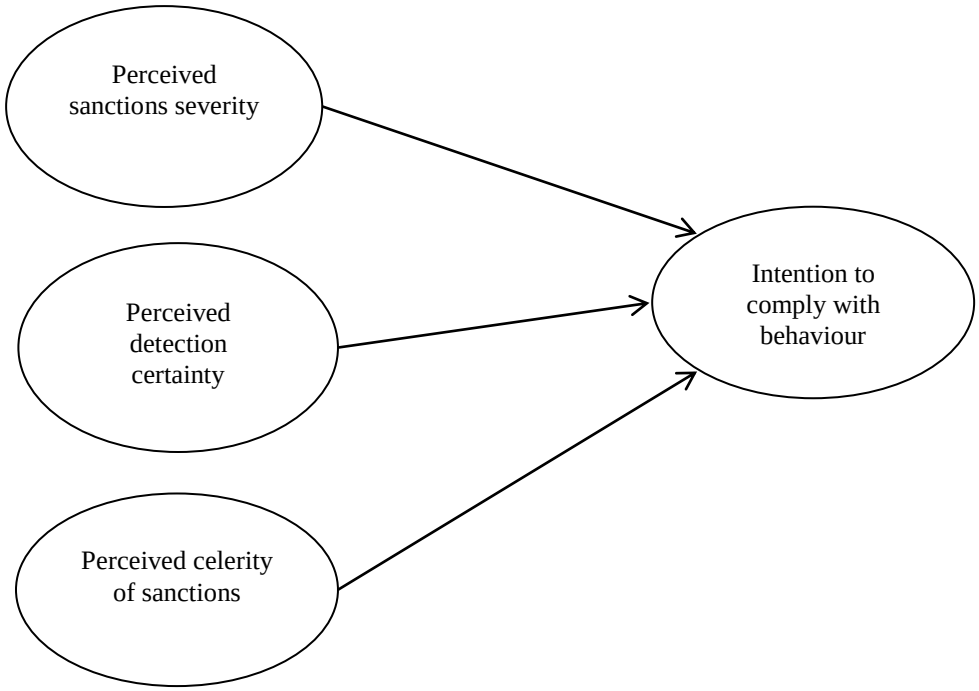


Figure 2.1: General Deterrence Theory (Hu, Xu, Dinev &Ling, 2011)

The GDT's theoretical framework has been used to explain the relationship between management decisions and organisation's investments in information security without modifying the theory (Straub, 1990). Other researchers modified the theory because the individual's behavioural intention to comply with acceptable information security behaviours could also be affected by other factors such as individual characteristics (for example, gender, age), computer self-efficacy and risk propensity (D'Arcy & Hovav, 2004; Gibbs, 1968; Weaver & Carroll, 1985).

For example, D'Arcy & Hovav, 2004 extended GDT by adding three variables: security countermeasures, employment context (permanent or temporary) and individual characteristics to study the context of IS security controls.

Individual characteristics and employment context moderate the relationship between organisational security countermeasures and the constructs of perceived sanctions severity and perceived certainty of sanctions.

In addition, other past researchers integrated the GDT with other theories such as PMT (Herath & Rao, 2009) to examine the information security policy compliance behaviours in organisations. PMT constructs were used to understand the attitude of end users with regard to information security policy compliance, while deterrence constructs (punishment severity and detection certainty) were used to understand the influence of deterrence mechanisms on information security policy compliance among the end users (Herath & Rao, 2009).

2.2.2 The Health Belief Model (HBM)

The theory was originally developed in 1950's in an attempt to understand why citizens were not interested in participating in free Tuberculosis (TB) screening (Hochbaum, 1958). The original constructs of the HBM include: (1) perceived susceptibility which is used to portray individual's judgment of the chances for suffering a certain disease; (2) perceived severity reflects an individual's perception of health seriousness that the person may face after contracting a disease, and how the disease would affect his or her lifestyle.

(3) Perceived benefits show an assessment of the benefits that could be gained by an individual after taking recommended actions from other people or

organisation or agency; and (4) perceived barriers to action reflects an individual's assessment of the perceived costs: financial and non-financial (such as inconvenience, pain and embarrassment) that the individual may face during the execution of a health behaviour.

Perceived susceptibility and perceived severity jointly forms perceived threat (Glanz, Rimer, & Viswanath, 2008; Janz & Becker, 1984; Rosenstock, 1974). Past researchers argue that individual's likelihood of taking a recommended action could be determined by the individual's evaluation of the relevant threats and cost-benefits. The original HBM is shown in figure 2.2.

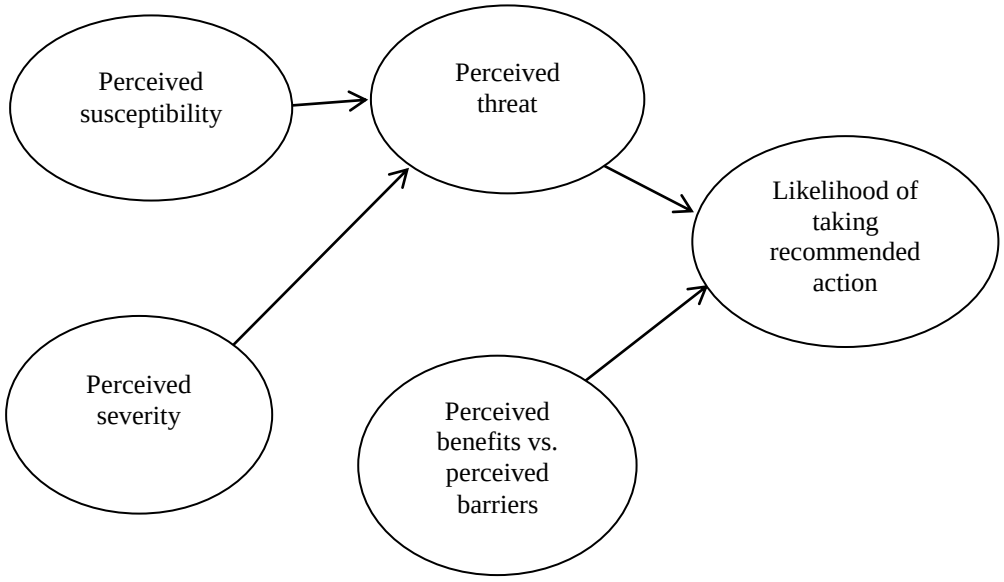


Figure 2.2 : Theoretical Framework of the Original Health Belief Model (Rosenstock,1966)

To increase the model's ability to measure health-related behaviours, Rosenstock (1966) extended the original model by including two constructs: cue to action and modifying factors.

Cue to action is either an internal or external stimulus factor (such as advice from credible or important people or institution) which motivates an individual to respond positively to a recommended action. While, modifying factors are related to individual's characteristics, namely (1) demographics: age, gender, race, ethnicity, and education; (2) psychosocial variables: personality, social class and peers and group pressure; and (3) structural variables: people's knowledge of the disease and prior contact with the disease. According to Rosenstock (1966), the effect generated by perceived threat, perceived benefits and perceived barriers on a person's likelihood of taking recommended action could be affected by the above modifying factors.

Later in the year 1988, self-efficacy was added as an additional construct since an individual's ability or competence to perform certain action could influence individual's likelihood to act (Glanz et al., 2008; Rosenstock, Strecher, & Becker, 1988). Rosenstock et al. (1988) assert that the inclusion of self-efficacy construct to the HBM would enhance the explanatory power of the model in explaining individual's differences in health behaviours. The Modified HBM is shown in figure 2.3.

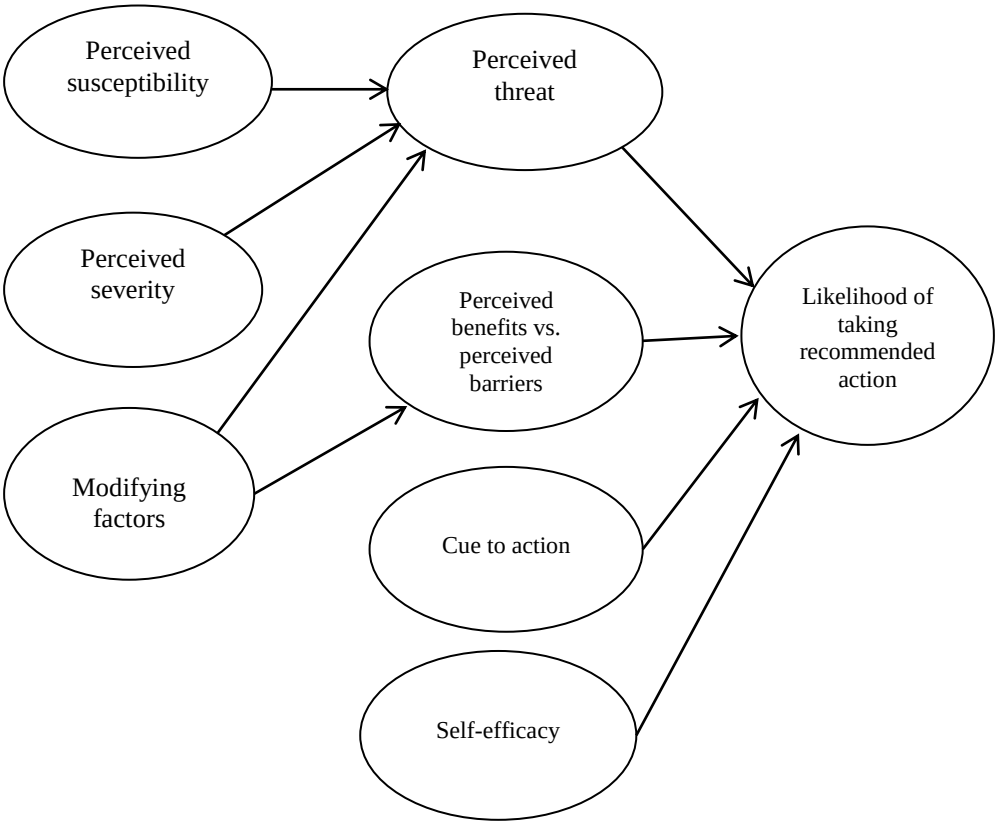


Figure 2.3: Theoretical Framework of Modified Health Belief Model (Janz & Becker, 1984; Rosenstock, 1974)

In recent years, interest in using HBM to study information security behaviours in IS domain has increased. For example, Claar and Johnson (2012) and Ng et al.(2009) used the model to explain information security behaviours of the users when dealing with adoption of information security software and e-mail attachments respectively. Davinson and Sillence (2010, 2014) applied the constructs of the model to investigate user's online information security perceptions when doing financial transactions and to promote user online secure behaviour respectively**.**

Humaidi and Balakrishnan (2012) used the model to develop a conceptual framework for studying the influence of information security awareness and information security technology on user's behaviour during deployment of health information system; while Yun and Arriaga(2013) used the model to develop an SMS-based health intervention for people suffering from asthma. In addition, Chuang, Tsai, Hsieh and Tumurtulga (2013) used the model for investigating the adoption of Telecare.

2.2.3 Protection Motivation Theory (PMT)

PMT was developed by Rogers in 1975 for the purpose of explaining ways (related to fear appeals) that can motivate individuals to avoid unhealthy behaviours. Later, the theory was extended into the more general theory that emphasises on cognitive processes which could mediate human behavioural change (Rogers, 1983).

PMT posits that the considerations of the following elements may influence an individual's intention to protect oneself against unhealthy behaviours. The first element refers to the intrinsic and extrinsic rewards that an individual would gain. An individual will then compare the perceived rewards (intrinsic and extrinsic) with (1) perceived severity that the person would be exposed or the extent in which the threat can cause harm; and (2) perceived vulnerability (Subjective risks an individual is exposed to). The difference between the perceived rewards, perceived severity, and perceived vulnerability will equate the individual's threat appraisal (Rogers, 1983).

On top of that, an individual will evaluate: (1) the effectiveness of response efficacy that needed to be carried out by to prevent an unwanted phenomenon from happening; and (2) individual's confidence and ability to execute a preventive behaviour, or defined as self-efficacy. The summation of an individual's (1) response efficacy effort and (2) self-efficacy that need to be devoted to forming a preventive behaviour that will equalise individual's estimation of the total response costs.

Such assessment of costs may eventually guide the person on how to react or respond to a perceived threat or termed as a coping appraisal (Rogers, 1983). After comparing the threat appraisal and coping appraisal, the person will be motivated to react (defined as protection motivation) and may eventually practice an action. The theoretical framework of the PMT is shown in figure 2.4.

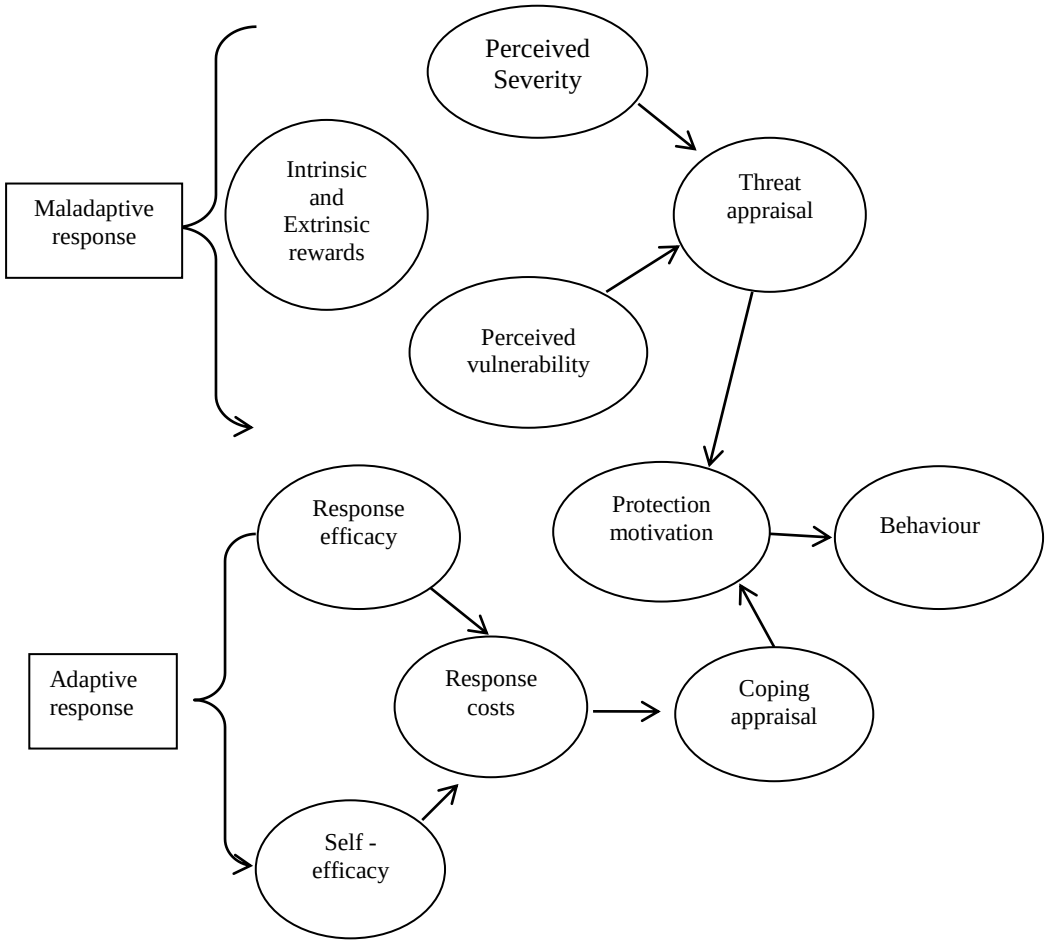


Figure 2.4: Theoretical Framework of Original Protection Motivation Theory (Rogers & Prentice-Dunn ,1997)

PMT has been used to explain a range of behaviours in IS domain, in particular, information security-related behaviours. The following authors, Herath and Rao (2009), Siponen et al (2006), Vance, Siponen and Pahnila, (2012) have used the theory to explain IS security policy compliance. The following modifications were done on the theory in their studies. Herath and Rao (2009) integrated PMT with GDT, TPB, Decomposed Theory of Planned Behaviour (DTPB) and the construct of organisational commitment.

Siponen et al (2006) introduced two variables: technology visibility and normative beliefs motivation process model to study its effects on perceived severity and perceived susceptibility of users of information systems on intention to comply with security policies. Vance, Siponen and Pahnila, (2012), have added security habits construct as a determinant of both maladaptive response (rewards, perceived severity and perceived susceptibility) and adaptive response (response efficacy, response costs and self-efficacy).

Further, PMT was integrated with Unified Security Practices (USP) theory to explain individual information security behaviours, in which the constructs of perceived severity, perceived susceptibility, response efficacy, response costs and self-efficacy were modelled as determinants of unified security practices: updating software, using passwords, firewall and performing data back-up) (Crossler & Belanger, 2014).

2.2.4 Theories of Reasoned Actions (TRA) and Planned Behaviours (TPB)

The theory of reasoned action (TRA) was developed by Ajzen and Fishbein (1980) to understand human attitude and intentions towards a specific behaviour. TRA posits that the intention to perform certain behaviours is determined by attitude and subjective norms. Individual's attitude or feelings (either positive or negative) would influence their decision on whether to perform or not to perform certain behaviours, while subjective norm would reflect the pressure exerted by social environmental factors such as pressure

from friends and relatives which may also influence an individual to perform certain behaviours (Pahnila et al., 2007). The theoretical framework of TRA is presented in figure 2.5.

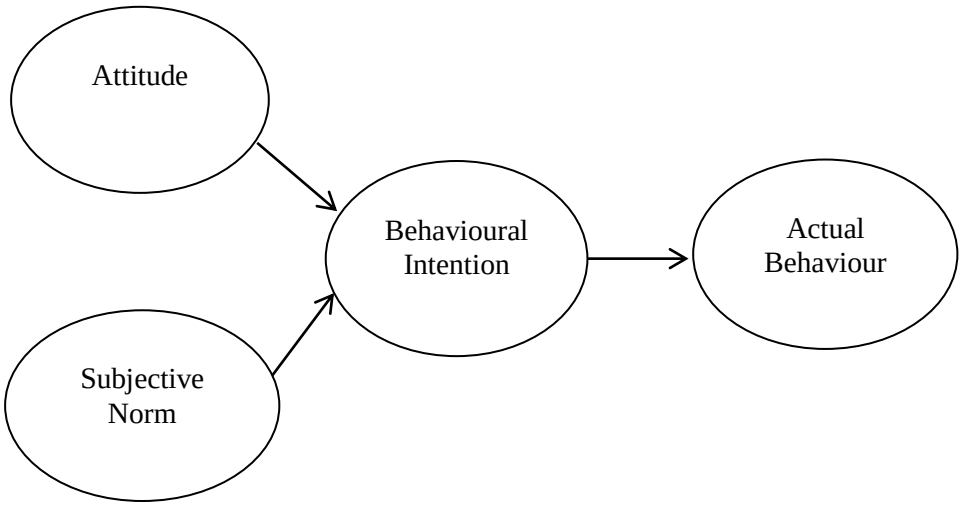


Figure 2.5: Theoretical Framework of Theory of Reasoned Action (Ajzen & Fishbein ,1980).

Theory of planned behaviour (TPB) was extended from TRA by including an additional construct: perceived behaviour control (PBC) (Ajzen, 1991). PBC is originated from Bandura's self–efficacy concept (Bandura, 1977) and is used to reflect an individual's perception on how easy or difficult for that individual to engage certain behaviours in his or her own capability. According to TPB, PBC is the key determinant for an individual to perform certain behaviours. In other words, an individual may not be able to perform certain behaviour in the absence of PBC, even though the effects created by subjective norms and attitude are strong (Theoharidou et al., 2005). Theoretical framework of PBC is presented in figure 2.6.

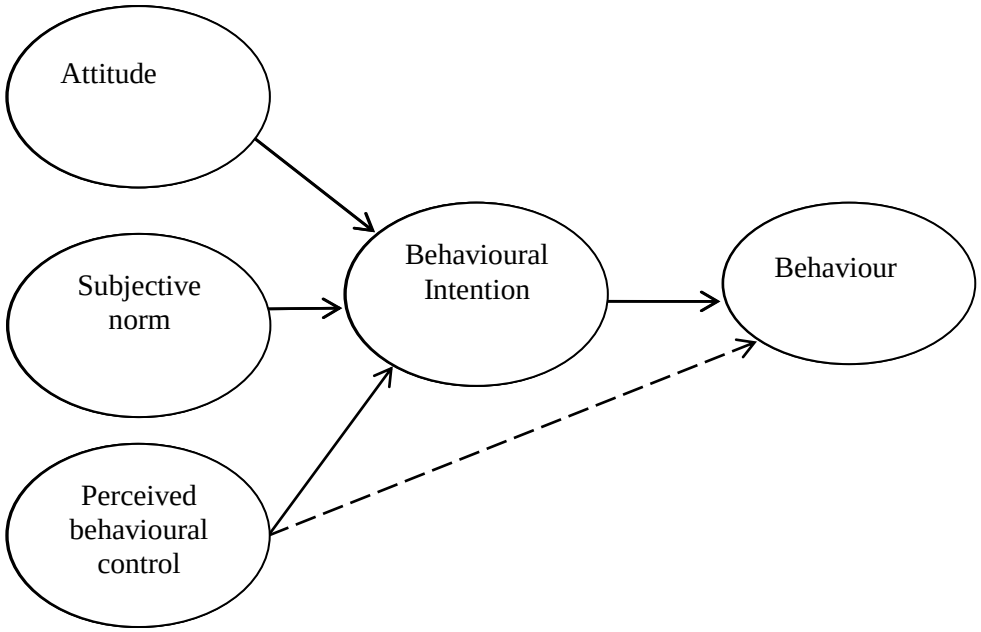


Figure 2.6: Theoretical Framework of Theory of Planned Behaviour (Ajzen , 1991)

Both theories (TPB and TRA) have been used widely in IS literature, notably in the context of this study. The past researchers have integrated the theories with other theories such as PMT to explain information security policy compliance in the organisation and intention to practice information security behaviour particularly on intention to use an updated anti-virus software (Ifinedo, 2012; Ng & Rahim, 2005).

2.2.5 Technology Threat Avoidance Theory (TTAT)

The theory was developed by Liang and Xue (2009) through the aggregation of insights that were derived from different fields of studies, ranging from health psychology, ICT management, marketing and risk analysis. Specifically, TTAT was developed from cybernetic theory (Edwards, 1992), coping theory

(Lazarus, 1993), expectancy theory (Steers, Mowday, & Shapiro, 2004), and cumulative theory (Tversky & Kahneman, 1974). Other elements in the TTAT were borrowed from risk analysis (Rogers & Prentice-Dunn, 1997) and health psychology (Rosenstock, 1966).

TTAT is used to explain why and how people avoid IT threats in voluntary settings (for example in a non-working environment) (Liang & Xue, 2010). In details, the theory posits that when individuals perceived a threat, would become motivated to avoid it actively by performing problem-focused coping or passively by performing emotion-focused coping. Problem–focused coping is performed when an individual believes that IT threat can be avoided by taking certain safeguarding measures such as using information security measures or anti-virus software to protect computer operating system. However, if the threat cannot be avoided, the person will opt for emotion–focused coping or an individual will prepare himself or herself to expect the worse. The technology avoidance theory is shown in figure 2.7.

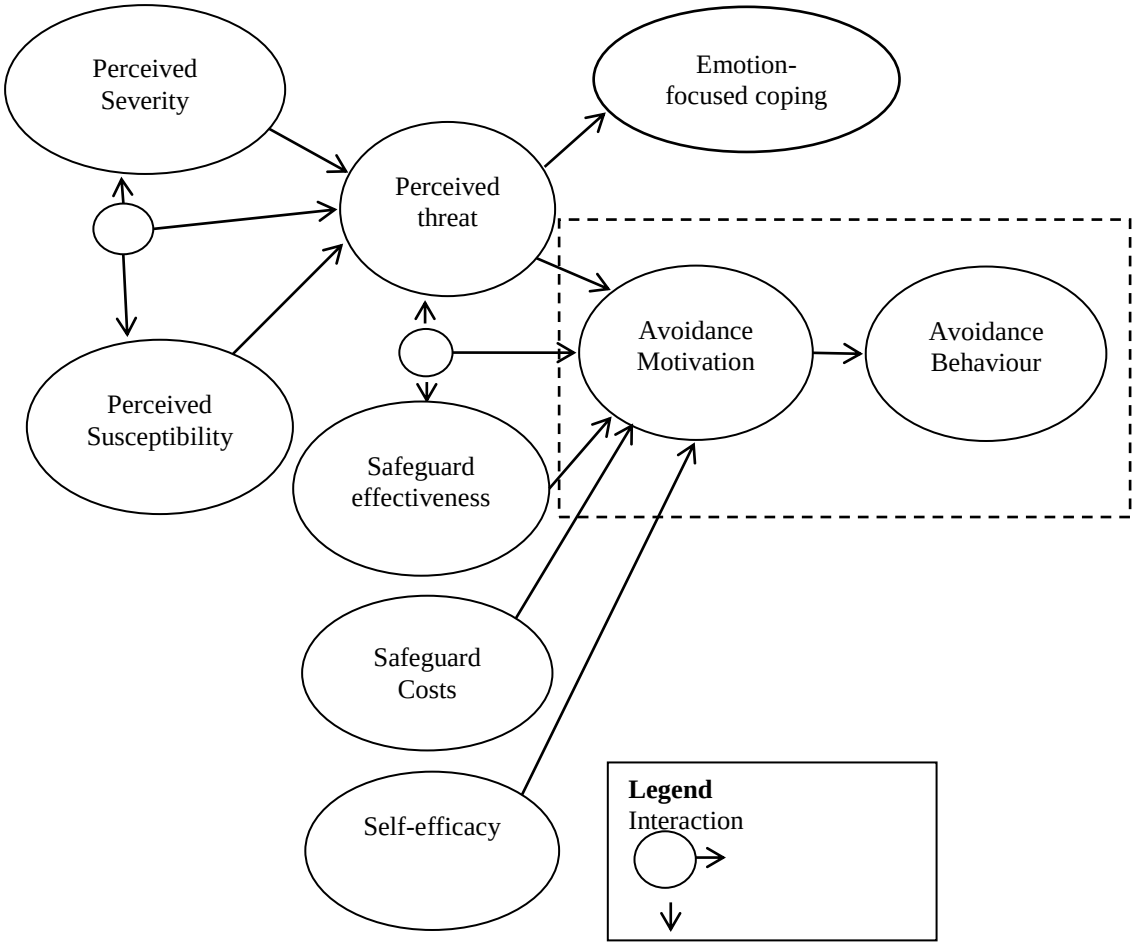


Figure 2.7: Technology Threat Avoidance Theory (Liang & Xue , 2009; 2010)

This theory was used in Liang and Xue (2010) to investigate IT threat avoidance behaviours of end users when using personal computers. The theory was used without any modifications.

2.2.6 Justification for Using the HBM

To solve the current study's research problems, HBM has been chosen over other theories because of the following reasons. The constructs of self-efficacy (which is measured by respondent's knowledge, skills and confidence to

practice information security behaviours) and cues to action (refers to the use of communication channels that may enhance respondent's awareness of information security threat) could address the issue of lack of information security awareness among government employees. (Abawajy, 2014; Bada & Sasse, 2014; Rhee, Kim, & Ryu, 2009). Although the construct of self-efficacy is found in other theories such as TTAT, PMT and TPB, the construct of cues to action is only found in the HBM.

Poor perceived susceptibility and severity of information security threats, benefits and barriers to execute information security behaviours among government employees can be addressed by the HBM constructs of perceived susceptibility, severity, benefits and barriers respectively. In addition, HBM can suitably be used to measure the influence of education level of government employees on intention to practice information security behaviours as compared to other theories. This is because the variable of education level and its underlying relationship with intention to practice information security behaviours is only found in HBM.

Theoretically, TTAT could serve as the research model of this study if integrated with the construct of cues to action. However, TTAT is more suitable fornon-working setting in which users of computer systems have an option to apply emotion –focused coping to security threats and are not bound to follow regulations and policies (Liang & Xue, 2009). In a work setting, a user is obliged to comply with regulations and security policies to avoid

security threats. On the other hand, the variables of GDT cannot address the research problem (see figure 2.1), hence cannot be used.

Although HBM was initially established to study problems related to health domain, the model has been widely used to study information security behaviour in information systems domain. For example, HBM was used to study information security behaviours in Claar and Johnson (2012) and Ng et al. (2009) studies, hence it is appropriate to be used in this study.

2.2.7 Summary of the Relevant Theoretical Frameworks in Information Security Behaviour

Literature in information security behaviours suggests that, the adoption of one information systems (IS) behavioural theory without extending or adding new variables or variable may not be used to explain the information security behaviour adequately. This is due to the inherent weaknesses of each behavioural theory. Therefore, many past IS researchers have integrated one or more behavioural theories used in the same or other research areas. For example, TPB was integrated with protection motivation theory (PMT) to study information security behaviour related to utilisation of protective information security technologies such as the use of anti-virus to protect computer systems (Ifinedo,2012). Initially, PMT was developed in the health care field to explain the role of fear appeals.

Later, PMT was extended to explain the cognitive processes that can mediate change of human behaviour (Rogers, 1983). Table 2.1 highlights strengths and weaknesses of the theories used in the past studies.

Table 2.1: A summary of Weaknesses and Strengths of Relevant Theoretical Frameworks

Theory	Weakness	Strengths
1. GDT	• Does not include unceremonious social processes of reward, moral and personal traits beliefs as part and parcel in predicting behaviour [a]	• A construct perceived sanctions has a remarkable influence in issuing criminal sanctions for unacceptable behaviours in a variety of areas of criminal sentencing [a]
2. HBM	• It does not take into account behaviours that are under non-conscious control [b] • The relationship between constructs was not clearly defined [c]	• Use simplified health-related constructs that are easy to understand and implement [c] • Provide cognitive determinants of a wide range of behaviours [d]
3. PMT	• Only some of its constructs (i.e. cognitive and environmental) have an effect on attitude change [e] • A small or moderate relationship is observed among perceived vulnerability, severity and behaviour [f].	• It is more effective in adherence interventions situations such as taking long-term medications [f]
4. TRA	• Assumes that human actions are under non-conscious control [h].	• Is powerful in identifying potential persuading targets that may influence a specific, willful behaviour [i] • Appropriately used in studying behaviour related to technology adoption [j]
5. TPB	• Does not take into account emotional factors [h]	• The perceived behaviour control explains reasonably well the relationship between the behaviour intention and the actual behaviour [k]. • Appropriately used in studying behaviour related to technology adoption [j]
6. TTAT	• Its applicability is limited to non-work settings and in investigation of behaviour of individual computer users [l]	• It is appropriately used in explaining threat avoidance-related behaviours [m].

Table 2.1 Continue next page

Source:

[a] Lieberman (2010)

[g] Stroebe (2011)

[b] Maguire (2010)
[c] Armitage and Conner (2000)
[d] Orji, Vassileva, and Mandryk (2012)
[e] Rogers (1983)
[f] Brewer et al. (2007)
[I] Montano et al. (2008)
[j] Oliveira and Martins (2011)
[k] Ajzen (1991)
[l] Liang and Xue (2010)
[m] Liang and Xue (2009)

2.3 Overview of Research Models that used HBM Theory

Most of the IS studies that had adapted HBM were carried in year 2000's (Claar & Johnson, 2012; Chuang, Tsai, Hsieh, & Tumurtulga, 2013; Davinson & Sillence, 2010, 2014; Humaidi & Balakrishnan, 2012; Ng et al., 2009; Yun & Arriaga, 2013). The above studies modified the HBM to address their research objectives. The modifications were carried out in three ways. Firstly, new variables were included into the model. For example, Ng et al. (2009) added two variables: organisation technical controls and security familiarity. Secondly, researchers have integrated HBM with other models, for example, Humaidi and Balakrishnan, (2012) integrated HBM with PMT.

Thirdly, previous studies have modified the original relationships of certain constructs. For instance, Chuang, Tsai, Hsieh and Tumurtulga (2013) challenged the direct relationship between cues to action and behavioural intention. Instead, the authors proposed that cues to action could mediate the effect created by perceived severity, susceptibility, benefits, barriers, cues to action and self- efficacy on intention to adopt telecare. In another study, Ng et al. (2009) hypothesised that perceived severity, in fact, could moderate the relationship between perceived susceptibility, benefits, barriers, cues to action and self-efficacy and at the same time perceived severity could generate direct

effects on intention to practice computer security behaviours. Meanwhile, Claar and Johnson (2012) asserted that modifying variables could serve as moderating variable instead of serving as antecedents' variable. A summary of relevant past studies research model that used the HBM along with the modifications that were done and the reasons behind those modifications is shown in table 2.2.

Table 2.2: A Summary of Past Research Models that used HBM

Model used	Modifications	Reasons for the modifications
Modified HBM [a]	Modifying variables were modelled as moderating variables	Based on the proposition that HBM assumes the existence of moderating relationship between independent variables and dependent variable by modifying factors
Modified HBM [b]	Cues to action was modelled as mediation variable between HBM constructs and dependent variable	Reasons were not stated.
Protection and Motivation Theory (PMT) and Modified HBM [c]	An integrated model, whereby PMT and HBM variables were grouped under two constructs and behaviour was treated as mediating variable	Reasons were not stated.
Modified HBM [d]	Organisation technical controls and security familiarity was added. Perceived severity was modelled as moderating variable between HBM constructs and the independent variable General security orientation was added	These variables were added as control variables and as a means to increase internal validity of the study. General security orientation to address security consciousness
Modified HBM [e]	No modification was done	
Modified HBM [f]	Studied on perceived susceptibility construct only	Perceived susceptibility it increases concerns about financial fraud and thus motivates users to act securely, that's why it was the only construct studied.

Table 2.2 Continue next page

Model used	Modifications	Reasons for the modifications
Modified HBM [g]	Studied only perceived severity and knowledge a sub- construct of modifying factors	Knowledge sub- construct was studied based on proposition education to paediatric patients may lead to improved health outcomes and perceived severity was studied on assumption that one way to increase perceived severity of asthma disease is through making patients aware of the symptoms of the disease.

Source:

[a] Claar and Johnson, (2012)
[b] Chuang, Tsai, Hsieh and Tumurtulga (2013)
[c] Humaidi and Balakrishnan, (2012)
[d] Ng et al. (2009)
[e] Davinson and Sillence (2014)
[f] Davinson and Sillence (2010)
[g] Yun and Arriaga, (2013)

On top of studying the modifications that were done by the past studies on the HBM, it is necessary to find out whether the current research can challenge the HBM's previous propositions. This is because some past studies that used HBM had produced consistent and contradictory results. For example, results generated by perceived susceptibility, perceived severity, self- efficacy and cues to action were consistent with Claar and Johnson (2012) and Ng et al (2009) studies. However, perceived benefits and perceived barriers generated contradictory results in both studies, whereby perceived benefits were supported by Ng et al (2009), but they were not supported by Claar and Johnson (2012). In addition, perceived barrier was not supported in Claar and Johnson (2012) as well as in Ng et al (2009).

Contradictory results with regard to perceived barriers and perceived benefits between the two studies were caused by the difference in characteristics composition of respondents. Respondents from Ng et al. (2009) study were computer savvy (i.e. part-time working computing students and individuals employed in IT-relatedorganisations) hence respondents had knowledge of the

benefits of practising information security behaviour and did feel that practising information security behaviour was not difficult, therefore not a barrier to them.

On contrary, respondents from Claar and Johnson (2012) study were home computer end users who have limited computer knowledge and ICT skills. Thereby, barriers such limited ICT skills could significantly affect their ability to perform information security behaviours. Meanwhile, respondents in Davinson and Sillence's (2014) study had purchased an insurance policy that would cover any possible loss that may occur during the e-transactions. As a result, they had little intention to practice information security behaviours. In brief, the HBM's original proposition could be challenged if the studied respondents possess specific characteristics such ICT knowledge.

The examination of effects created by perceived severity, susceptibility, benefits, barriers; cues on intention to practice information security behaviours are common in information security studies. Nevertheless, studies that have comprehensively investigated the problems related education level and information security habit are limited.

One of the main reasons for the limitation of studies on information security habit studies could be related to the level of ICT development among the studied countries. The studies of Claar and Johnson (2012), Davinson and Sillence (2014) and Ng et al. (2009) were carried out in developed countries: United States of America (USA), United Kingdom (UK) and Singapore

respectively. These developed countries are among the leading countries in the e-Government system development index while Tanzania is ranked in middle e-Government development index (EGDI), the USA, UK and Singapore are in ranked in very high e-government development index (UN, 2016). As habit can be learned over time by experiencing and correcting the misconducts (Triandis, 1979), people in developed countries thereby would have become better on information security habits. As a result, studies that examined information security habits in developed countries are limited because the respondents are expected to practice acceptable security habits.

2.3.1 Relevant Past Study's Measurement Items

Past studies have measured perceived severity, susceptibility, benefits, barriers, cues, self-efficacy, information security habits, behavioural intention and actual practice of information security behaviours (see table 2.3). Overall, past studies used three or more measurement items borrowed from the past studies in IS field or other relevant fields to measure a single construct (see table 2.3).

As most of the past studies have tested the measurement item's reliability and/or validity, this study thereby has considered all items suggested by the past researchers to measure the relevant variables. Nevertheless, the items were carefully screened to ensure that the measurement concept of each item is not overlapping. The screening process was conducted by IS experts in which items that share similar meaning or concept were grouped together. Relevant

measurement items before screening are reported in table 2.3. Screened items are reported in table 3.4, page number78.

Table 2.3: Relevant Constructs and Items used in the Past Studies

Constructs and its Measurement Items
Perceived Severity
1. If my computer were infected by malicious software as a result of using suspicious, untrusted and unsecure sites it would be severe [a]
2. If my computer were infected by malicious software as a result of using suspicious, untrusted and unsecure sites it would be serious [a]
3. If my computer were infected by a malicious software as a result of using suspicious, untrusted and unsecure sites it would be significant [a]
4. It would be severe if my computer were affected by malicious software as a result of using suspicious, untrusted and unsecure sites [b]
5. Having the data in my computer stolen by malicious software as a result of using suspicious, untrusted and unsecure sites would be a serious problem for me [c]
6. Losing data as a result of malicious software would be a serious problem for me [c]
7. Malicious software such as spyware would steal my personal and Organization information from my computer without my knowledge [d,f]
8. My personal and Organisation information collected by malicious software as a result of using suspicious, untrusted and unsecure sites could be misused by cyber criminals [d]
9. My personal and office information could be collected by malicious software and sent to third parties [d]
10. My personal information collected by malicious software as a result of using suspicious, untrusted and unsecure sites could be used to commit crimes against me[d]
11. Malicious software would make my computer run more slowly [d]
12. Malicious software would crash my computer system from time to timed
13. Malicious software would affect some of my computer programs as result of using suspicious, untrusted and unsecure sites and make them difficult to use**. [d]**
Perceived Susceptibility
14. My computer is at risk for becoming infected with malicious software as a result of using suspicious, untrusted and unsecure sites [a]
15. It is likely my computer that will become infected by malicious software as a result of using suspicious, untrusted and unsecure sites [a, i]
16. It is possible that my computer will become infected with malicious software as a result of using suspicious, untrusted and unsecure sites [a]

Table 2.2 Continue next page

Constructs and its Measurement Items
17. There is a chance that Organization information will be disclosed by malicious software as a result of using suspicious, untrusted and unsecure sites [e]
18. Data on my computer are likely to be damaged by malicious software as a result of using suspicious, untrusted and unsecure sites [j]
19. Chances of being infected malicious software as a result of using suspicious, untrusted and unsecure sites are high [b]
20. There is good possibility that I will be infected with malicious software as a result of using suspicious, untrusted and unsecure sites [b]
21. I am likely to be infected with malicious software as a result of using suspicious, untrusted and unsecure sites [b, i]
Perceived benefits
22. Being cautious in using online resources such as websites is effective in preventing malicious software from entering my computer [b]
23. Checking if trusted and secure site make sense is effective in preventing spyware from entering my computer [b]
24. Checking if the website is trusted and secure site make sense is effective in preventing malicious software from entering my computer [b]
25. If I prevent malicious software from entering my computer, I would improve my productivity [g]
Perceived Barriers
26. Checking if the website is trusted and secure would complicate the way I use my computer [h]
27. Checking if the website is trusted and secure effectively is time-consuming[h, I,]
28. Checking if the website is trusted and secure would entail significant determination other than time [b, h]
29. Checking if the website is trusted and secure is inconvenient for me [e]
30. Too many overheads are associated with checking if the website is trusted and secure [e]
Cues to Action
31. If I see a report, or read a newspaper concerning a new computer threat, I would be more concerned about my computer's probability of being hacked [h]
32. If I receive an email from the computer software vendor concerning a new information security vulnerability, I would be more worried about the probability of being hacked [h]
33. If a work mate could inform me of the latest experience with a malware, I would be more conscious of my computer's probability of being hacked [h]
34. If I receive reminders from my organisation about information security attacks, I would be more vigilant [h]
35. My Organisation distributes information security newsletters [b]

Table 2.3 Continue next page

Constructs and its Measurement Items
36. My Organisation sends out message concerning information security [b]
37. My Organisation constantly reminds me to practice acceptable computer security actions [b]
Self- Efficacy
38. I am confident to identify suspicious, untrusted and unsecure sites without much effort [b, h]
39. I can find information I need if I encounter difficulty in identifying suspicious, untrusted and unsecure sites [h, b]
40. I am confident that I can identify suspicious, untrusted and unsecure sites [b]
41. I have knowledge and ability to protect my personal and organisation data from external threats [f]
Information Security Habits
42. Removing malicious software the habit for me [k]
43. I should automatically check for suspicious, untrusted and unsecure sites before accessing them [j]
44. I should periodically remove malicious software [j]
45. Checking for suspicious, untrusted and unsecure sites before accessing them is something I do without having to consciously remember to do so. [e]
46. Checking for suspicious, untrusted and unsecure sites before accessing them is something that belongs to my daily routine [e]
47. Checking for suspicious, untrusted and unsecure sites before accessing them is something that I start doing before I realise am doing it. [e]
48. Checking for suspicious, untrusted and unsecure sites before accessing them is something that I feel weird if I do not do it [e]
49. I don't even think before checking for suspicious, untrusted and unsecure sites before accessing them. [k]
Intention to Practice Information Security Behaviours
50. I will actively check for suspicious, untrusted and unsecured sites as a precaution before accessing them [f, k]
51. I will take precautions against information security violations i
52. I will never open suspicious, untrusted and unsecured sites on my computer [j]
53. I certain that I would check for any suspicious, untrusted and unsecured websites or emails before accessing them [d, l.]
Actual Information Security Behaviours
54. I do check for the suspicious, untrusted and unsecure websites or emails to ensure that the websites or emails were not from fraudulent sources [d]
55. Sometimes, I don't check the suspicious, untrusted and unsecure sites if it affects my performance or productivity [i]

Table 2.3 Continue next page

Constructs and its Measurement Items
56. I do check the suspicious, untrusted and unsecure websites or emails ONLY when it is convenient for me to do so [d, i]
57. When I am busy, I don't check whether the suspicious websites/ emails were from fraudulent or scammed source [i]

Sources

[a] Johnston and Warkentin (2010)
[b] Ng et al. (2009)
[c] Woon et al.(2005)
[d] Liang and Xue (2010)
[e] Vance et al.(2012)
[f] Workman et al. (2008)
[h] Claar & Johnson (2012)
[I] Chan, Woon, & Kankanhalli (2005)
[j] Yoon et al. (2012)
[k] Limayem et al. (2004)
[l] Ifinedo(2012)

2.4 Overview of the Past Studies' Research Methodology

Claar and Johnson (2012) and Ng et al. (2009) employed quantitative research approach. This approach is suitable when the research is deductive in nature. Since the effects of studied constructs have been widely tested by many researchers, and in many study's locations and research domains, the above studies analysed the collected data to confirm the HBM theory or model's hypotheses.

On the other hand, qualitative approach is suitable for inductive research in which a theory is built up to explain the relationships between the studied variables. For example, Davinson and Sillence, (2014) and, Yun and Arriaga, (2013) collected qualitative data to better understand the other possible relationships that can be generated between perceived susceptibility, severity, benefits, perceived barriers, cues to action, self-efficacy and perceptions of being secure when doing online transactions. Since the current study is the

deductive research that intends to test and confirms a theory's hypotheses, quantitative approach thereby is appropriate.

Past studies suffer from two major limitations emanated from using online tools to collect data (Claar & Johnson, 2012; Davinson & Sillence, 2010) and the inadequate sample size, for example (Claar & Johnson, 2012; Ng et al., 2009). The online survey may not be suitable because:

(1) The data validity is debatable, for example, relatively little may be known about respondent's characteristics in online communities. In addition, some private firms (such marketing and research firms) provide access to specialised populations to researchers in reference to data from past surveys. However, if the research data were collected using the self-reported instruments, there is no assurance that the respondent from past surveys provided accurate demographic or characteristics information. Therefore, there is the possibility of sourcing the wrong respondents, which may result in sampling error.

(2) Sampling from the list of emails may also be challenging due to multiple email addresses for the same person and invalid/inactive emails (Andrews, Nonnecke, & Preece, 2003; Couper, 2000). For example, one respondent with two different emails can be selected to participate in the study or a selected respondent failed to receive an email due to inactive or invalid email address.

(3) In addition, people tend to ignore online survey due to some few reasons: they may suspect emails invitations to participate in a study as irrelevant or unsolicited information (spam) (Andrews et al., 2003), or an offensive behaviour, in which a potential participant may think that the survey link or an email may contain hatred or hurtful contents (Hudson & Bruckman, 2004).Therefore, the targeted population may refuse to participate. Collectively these limitations may mislead the researchers to make wrong conclusion about the findings (Wright, 2005).

After reviewing the limitations of online survey highlighted above, the current researcher noted that online survey should not be used in this study because of its limitations and the difficulty to establish or obtain the list emails for Tanzanian government employees with the required characteristics for the study. However, similar to Ng et al (2009), the current study employed the traditional paper and pencil questionnaire in order to avert the above-stated limitations. Contrary to Ng et al (2009), small token was not given as an incentive to encourage respondents to respond. Tanzania government employees are not allowed to accept any gift or any form of an incentive unless it is declared and approved by the authorities. In such circumstances, it was difficult to encourage respondents using any form of incentive. Instead, the current study usedfollow-up calls to remind and encourage them to respond.

The results developed from small sample sizes (such as in the studies conducted by Claar and Johnson (2012), and Ng et al.'s (2009) survey) could be questionable because the data findings may not be able to represent the study population. For example, Claar and Johnson (2012) used the sample size of 184 respondents drawn from unknown population of home computer users responsible for the implementation and maintenance of security software. Using the formula for calculating sample sizes for the undefined (unknown) population (see Cochran (1977)), the minimum sample size could be in the range of 270 to 541 depending on the confidence level, margin error and the confidence interval set by the researcher.

On top of that, methodologies that could have been undertaken to ensure the representativeness of the sample to population were not disclosed in their articles. To ensure data representation, sample size should be large enough to represent the general population of the study and should be selected using a probability sampling technique (Davern, 2011; Yang, Wang, & Su, 2006). Most of the previous studies used non-probability sampling techniques (such as purposive and snowball sampling) see table 2.4. To ensure the sample size is representative, this study used Cochran formula to calculate its sample size (Cochran, 1977) and used stratified random sampling to select respondents. Further details with regard to current data collection method, determination of sample size are reported in chapter 3. The summary of past studies research methodologies with their limitations is shown in table 2.4.

Table 2.4: Summary of Past Studies Research Methodology

Literature	Approach	Respondent	Research tools	Sampling Technique	Sample size	Study's Limitations
Claar and Johnson (2012)	Survey	All home computer users in the USA	Questionnaire distributed via surveyshare.com	Snowball	184	• Study population is large and undefined [a] • Non- response bias may occur due to sampling technique used and anonymous nature of data collection [a]. • The application of online surveys may limit respondent choice of method of completing the survey [a]
Ng et al. (2009)	Survey	Part-time working IT students and IT employees	Questionnaire	Purposive	134	The study population consisted only of IT savvy respondents. Inclusion of not- IT savvy may yield different results
Davinson and Sillence (2010)	Survey and experiment	Staffs and students	A questionnaire distributed via survey monkey and paper based.	Purposive	64	The use of self- report data is prone to errors, reporting what they are supposed to act rather than their actual behaviour
Davinson and Sillence (2014)	Qualitative	North East of England residents	Semi- structured interview	Purposive	29	Small sample size may result in missing many effects of a construct on the dependent variable [c].
Yun and Arriaga (2013)	Qualitative	Asthma patients	Interview	Randomly selected	30	Small sample size may result in missing many effects of a construct on the dependent variable [c].

Source:

[a] Claar and Johnson (2012)
[b] Ng et al. (2009)
[c] Cohen (2013)

2.5 Overview of Relevant Past Studies' Data Analysis

The review of the literature on data analysis indicated that past studies employed both quantitative data analysis techniques (Claar & Johnson, 2012; Davinson & Sillence, 2010; Ng et al., 2009), and qualitative data analysis techniques (Davinson & Sillence, 2014; Yun & Arriaga, 2013). Specifically, Claar and Johnson (2012) and Ng et al. (2009) used moderated multiple regression (MMR) to study the effects of moderating variables on the relationships between independent variables and a dependent variable. Davinson & Sillence (2010) used mixed design ANOVA with repeated measures to examine behaviour at each stage of the study. Davinson and Sillence, (2014) and, Yun and Arriaga, (2013) both used thematic analysis.

Data analysis technique used by Davinson and Sillence (2010) was different from the one used by Claar and Johnson, (2012) and Ng et al. (2009) although both studies measured the influence of HBM constructs on information security behaviours. This difference is due to the nature or focus of the study. Davinson and Sillence (2010) study focused on monitoring the influence of perceived susceptibility construct over time. Mixed design ANOVA was, therefore, appropriate since it is used for monitoring changes over time and more efficient in determining significant effects (Krueger & Tian,2004).

In comparison, Claar and Johnson, (2012) and Ng et al. (2009) studies focused on measuring the moderating relationship between HBM variables, thus MMR was appropriate in that context. The summary of the overview of the past studies data analysis is shown in table 2.5. However, the application of MMR in the current study is inappropriate since this study does not measure moderating effects rather it is measuring a direct and indirect effects. Theoretically, multiple regressions can be employed in this study. However, it suffers from the ability to address measurement errors. The presence of measurement errors may attenuates correlations between the measured items and cause unstandardized regression weights of the variable to vary considerably. Variations in unstandardized regression weights will eventually affect the final results (Hayduk, 1987).

Comparably, structural equation modelling (SEM) techniques uses latent variables which disattenuates measurement errors and therefore allows estimation of the actual relationships between the variables under investigation (Bollen, 1989b). The study conducted by Blanthorne, Jones-Farmer and Almer, (2006) to illustrate effects of measurement errors using multiple regression techniques and SEM on the same data, found that the p- values and unstandardized regression weights varied considerably. Following the limitations of the past study's quantitative data analysis, this study deployed SEM technique to analyse data.

Table 2.5: Summary of Relevant Past Studies Data Analysis Techniques

Literature	Analysis Technique	Strengths	Weaknesses
Claar and Johnson (2012)and Ng et.al. (2009)	Multiple regressions	Appropriate in measuring correlations among variables [a]	Unable to accommodate measurement errors and unable to phenomena that are non-observable [b,c,d]
Davinson and Sillence (2010)	Mixed design ANOVA	Appropriate in measuring means and monitoring changes over time and more efficient in determining significant effects over time [d]	Unable to accommodate measurement errors [a]
Davinson and Sillence, (2014) and, Yun and Arriaga, (2013**)**	Thematic Analysis	Is flexible and can provide a rich and detailed information on the meaning of data	There are no clear guidelines to conduct thematic analysis

Source:

a Kline (2005)
b Liu (1988)
c Raykov and Marcoulides (2012)
d Krueger and Tian (2004)

Davinson and Sillence (2014) and, Yun and Arriaga, (2013) both studies used thematic analysis (a qualitative data analysis technique) to analyse data. Themes were derived from the constructs of the HBM and coded from interviews to identify and analyse patterns from the collected data. The meaning of the data, in the thematicanalysis, is deduced from the patterns of data collected (Braun & Clarke, 2006). Qualitative data analysis techniques can be used along with quantitative data analysis techniques in order to;(1) to confirm or cross- validates the results (2) to explore findings that have been analysed by qualitative techniques (Creswell & Clark, 2007). For example, non-significant results of self-efficacy on intention to practice information security can be explained by interviewing respondents to give the possible reason for the findings.

In summary, the two data analysis techniques can be used to augment the weakness of each technique. However, this study did not use the qualitative technique to analyse data because of time and financial constraints.

2.6 Summary of Literature Review

HBM has been widely used to explain human behaviour in different contexts. However, the application of HBM in information security behaviour studies is relatively new, started from the year 2009. Although the original HBM was vastly modified in four different ways (see section 2.3), the modifications are still not sufficient to address in full of current research's problems.

The original and modified HBM constructs can only be used to address the issue of lack of information security awareness, skills, poor perceived susceptibility and severity of security attacks, poor perceived benefits of practising acceptable security behaviours and barriers, while poor information security habit among government employees cannot be addressed. Besides, existing HBM's constructs may not be able to address non-conscious behaviour such as habit. On top of that, existing HBMs do not explain whether individuals' behavioural intention could lead to their actual performance. Therefore, the current researcher extends the HBM by adding additional variables: information security habit and actual information security behaviour.

Similar to past studies, the current study is using quantitative research approach. Quantitative research approach can appropriately address the objectives of the current study. The current researcher also noted that, most of the data analysis methods used in the past studies may not able to address the issue of measurement error. Measurement errors may mislead researchers to make wrong conclusions about study's results. Thus, other data analysis technique such as SEM could be more useful as the method can handle measurement errors relatively better than other data analysis methods.

The past HBM-based researches tended to study only the conscious factors, where users were assumed to be rational: i.e. they were able to make their decision consciously and willingly (Henderson, 2005). In other words, users may conduct a cost-benefit analysis before performing certain behaviour. Nevertheless, some literature also suggest to include the study of habitual factors (Pahnila et al., 2007; Ouellette & Wood, 1998), where users may perform certain act automatically or unconsciously (Pollard, 2005). In line with the literature, this study examined both conscious and non-conscious behaviours in the present research framework.

2.7 The Proposed Research Framework

This study adopted the modified HBM as the foundational research model. The current study's research model consists of the following independent variables from the modified HBM: perceived susceptibility, severity, benefits, barriers,

and cues to action, self-efficacy, modifying factor (education level), and employee's intention to practice information security behaviours.

Nevertheless, the modified HBM was extended so that the current research issues can be addressed better.

HBM posits that behaviours are always under conscious control but in reality, most of the behaviours are determined by individual's habits (i.e. under non-conscious control) (Taylor et al., 2007). Therefore, to empower HBM to address poor information security habits observed from Tanzania government employees, information security habits construct was added to the HBM. In the context of this study, information security habit is defined as a form of distinct actions that are learned and practised by individuals without their conscious control and which requires little mental efforts to perform (Bargh, 1994; Verplanken & Aarts, 1999; Wood & Neal, 2007). Typical examples of information security habits are locking a personal computer (PC) every time before leaving an office desk or scanning an external device before opening its contents. Information security behaviour includes actions or behaviours which are controlled by explicit evaluations of an action and conscious mind (Dinev & Hu, 2007;Vroom & Von Solms, 2004).

On top of that, the variable that reflects respondent's actual performance of information security behaviours was also added. This is due to the fact that government employees are the ones with the responsibility of operating e-government systems. Therefore, understanding their actual information

security behaviours is imperative for effective management of information security management for the e- government information systems.

In both, the original and modified HBM, perceived susceptibility and perceived severity were assumed to be the antecedent factors of perceived threat (see figure 2.2 and 2.3). However, previous studies argue that treating the construct of perceived threat as a direct predictor of the behavioural intention is inappropriate as this may disturb the expectancy value of the HBM (Sheeran & Abraham, 1996). Further, previous studies found that both perceived susceptibility and perceived severity were, in fact, generating a direct effect on behavioural intention (Claar, 2011; Claar & Johnson, 2012; Ng et al. 2009; Orji, Sheeran & Abraham, 1996; Vassileva, & Mandryk, 2012). Therefore, in this study, the constructs of perceived susceptibility and perceived severity are treated as independent variables.

According to the modified HBM, modifying factors (such as age, gender, education levels, race, ethnicity and religion) could indirectly affect the intention to perform behaviours through individual's perceptions of threats (susceptibility and severity), perceived benefits, and perceived barriers (Janz & Becker, 1984). Thus, in line with the modified HBM and the past study's propositions, the current study suggests that the following variables: perceived susceptibility, severity, benefits and barriers could mediate the effects generated by education level (modifying factor) on respondent's intention to practice security behaviours.

Selection of modifying or demographic factors to study, depends on the research objectives or purpose of the study as indicated in the following past studies, Lévesque, Fernandez and Batchelder (2017), Oliveira et al. (2017), Reyns (2013) and Rundall and Wheeler (1979). In agreement with the previous studies, this study selected education level among the other modifying factors because one of the objectives of this study is to examine whether the level of education qualification among the government employees could influence the intention of the employees to practice information security behaviours. Education level is the key determinant factor when recruiting new employees. In addition to that, Furnell and Clarke (2005) argue that the level of information security training offered to users of information systems may differ between employees with different levels of education qualifications and background. Thus, to ensure the government employees could perform good information security practices when using e-Government information systems, the delivery of the training materials may need to be customised according to the employee's education level (PCI, 2014).

According to Becker, Maiman, Kirscht, Haefner, and Drachman (1977) and Janz and Becker (1984), the constructs of perceived benefits and perceived barriers should be weighed against each other. However, no guidelines were developed to facilitate the comparison between the two constructs. As the comparison between the two constructs could be difficult to estimate; previous studies suggested to study the two construct separately (Claar & Johnson, 2012; Ng et al., 2009; Ali et al., 2011; Cheney & John, 2013; Sharafkhani, Khorsandi, & Shamsi, 2014). Similarly, this study estimates the effects of

perceived benefits and perceived barriers on intention to practice information security behaviours as two separate independent constructs. The constructs of self-efficacy and cues to actions were operationalized as a direct predictor of intention to practice information security behaviour similar to the original and modified HBM. The current research framework and definitions of the constructs are shown in figure 2.8 and table 2.6 respectively. Additional variables are represented with bolded circles.

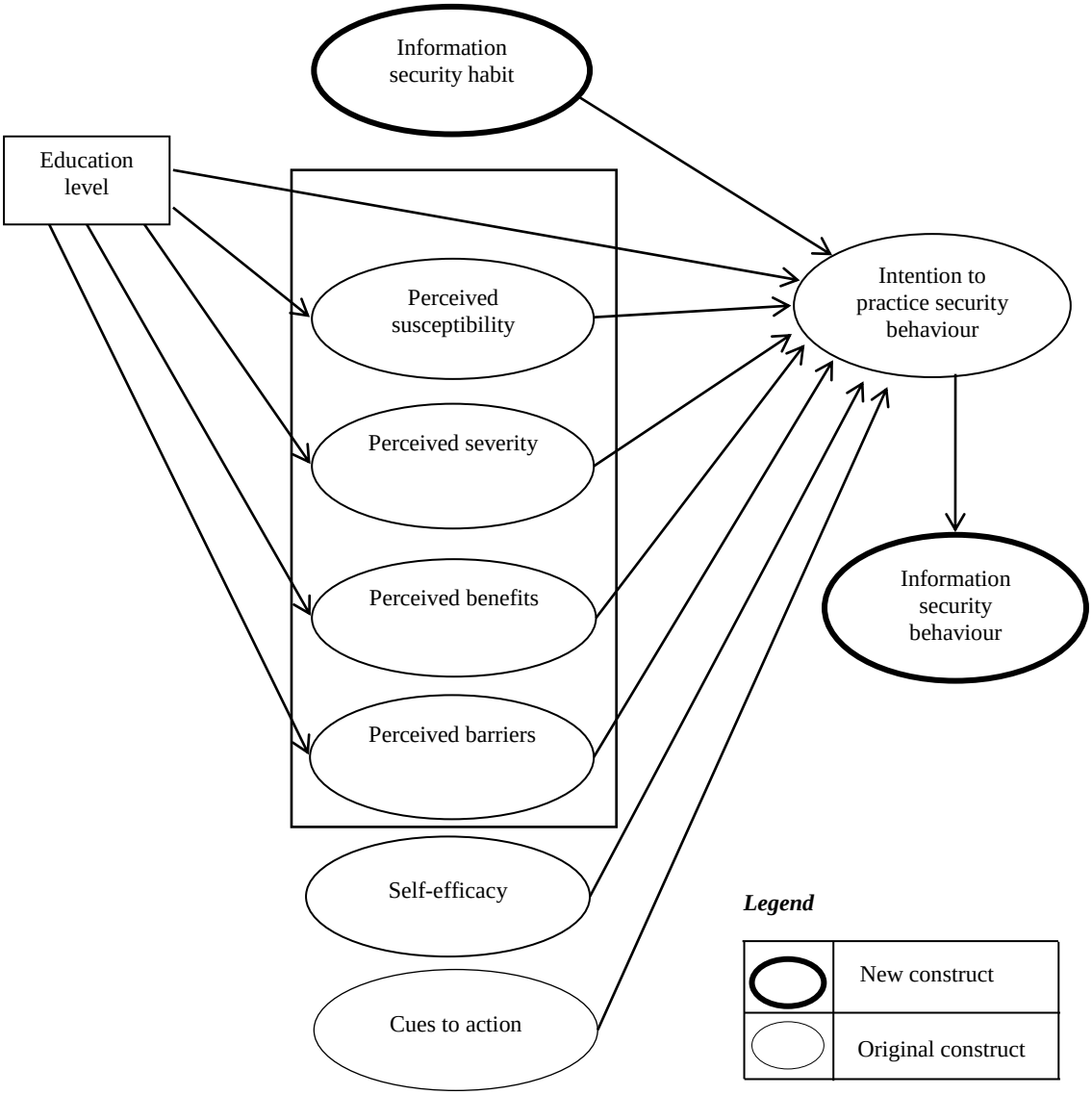


Figure 2.8: Current study's Research Framework

Table 2.6: Definitions of the Constructs of the Study

Construct's name	Definition
Information security habits	Includes security actions that are learned and executed without individual's awareness control (automatic) and requires little mental efforts. [a, b]
Perceived susceptibility	Refers to employee's belief with regard to vulnerability of an organisation to information security threats. [c, d]
Perceived severity	Is defined as the consequences an individual may experience as a result of security attack to the organisation information resources. [c, d, e]
Perceived benefits	Refers to the advantages an individual may gain as a result of practising acceptable information security actions. Such as preventing malicious software from affecting my computer my increases work productivity. [a, d, e]
Perceived barriers	It is described as employee's estimation of hardship or difficulty related to personal and environmental obstacles to performing acceptable information security actions. [a, d, e]
Self-efficacy	Refers to individual ability, knowledge and confidence to execute acceptable information security actions. [a, d, e]
Cues to action	Includes security alerts, messages, social influence, and information from work mates, software vendors and posters that motivate employees to perform acceptable information security actions. [a, d, e]
Education level	The highest level of education qualification attained by an employee. [f]
Intention to practice security behaviour	Likelihood of an employee to practice acceptable information security behaviours. [g, h]
Information security behaviour	The actual practice of information security behaviour, such as checking for suspicious, untrusted and unsecure websites or online resources before accessing. [i]

Table 2.6 continue next page

Source:

[a] Triandis (1979)

[f] OECD (2003)

[b] Verplanken and Aarts (1999)
[c] Claar and Johnson (2012)
[d] Ng et al.(2009)
[e] Liang and Xue (2010)
[g] Ajzen (1991)
[h] Hsu and Huang (2010)
[I]Stanton, Stam, Mastrangelo and Jolton (2005)

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Introduction

This chapter presents research methods and procedures that were used to test the current study's research model and the related hypotheses. The chapter proceeds by explaining the development of study's research hypotheses, research design, research instruments development and data analysis techniques used.

3.2 Development of Current Research's Hypotheses

The current study's research model has added information security habit as a new construct. Literature in nutrition studies indicates that an individual's habit is highly correlated with the intention to consume: (1) milk (Saba, et al., 1998), and (2) food containing fats (Saba, Vassallo & Turrini,2000). The past studies also showed that intention to use (1) condom among university students (Trafimow ,2000), and (2) ecstasy (Orbelll, Blair & Essex ,2001) was closely associated with the individual's habit. IS researchers have been predicting the similar positive relationship between individual's habit and behavioural intention (Baptista & Oliveira, 2017; Hong, Thong, Chasalow, & Dhillon, 2011; Jia & Hall, 2014; Lankton, McKnight, & Thatcher, 2012; Liao, Palvia, &

Lin, 2006; Masa'deh, Tarhini, Mohammed, & Maqableh, 2016). Hence, based on the past studies propositions, the current study expects that:

H1: Information security habits would increase employee's intention to practice information security behaviours.

Health care literature argues that modifying factors such as education could generate both direct and indirect effects (indirect effects is through perceived susceptibility, severity, benefits and barriers) on individual's intention to engage in health behaviours (Janz & Becker, 1984; Kegeles, Kirscht, Haefner & Rosenstock, 1965 ; Rundall & Wheeler, 1979). With regard to direct effects of education level on intention to practice behaviours, Rundall and Wheeler (1979) argued that individual's intention to visit their physician for medical check-up positively correlate with their academic qualifications.

Previous studies in IS also found that individuals with higher education level are more likely to perform certain information security actions or behaviours such as avoiding phishing attacks (Sheng et.al., 2010) and adopting internet and ICT in general (Birba & Diagne, 2012; Or & Karsh, 2009). In addition, personal characteristics such as the level of education could influence individual's intention to comply with organizational information security policies (Zhang, Reithel, & Li, 2009). Therefore, the current study predicts that:

H2: The level of education qualification could influence employee's intention to practice information security behaviour positively.

In discussing the indirect effects caused by education level on an employee's behavioural intention to practice information security, it is necessary to find out which constructs are playing the mediating role. Let's begin by identifying the role that could be played by the constructs of perceived susceptibility and perceived severity. Rundall et al. (1979) and Strecher and Rosenstock (1997) suggested that individuals with higher education level have higher perceived susceptibility to health-related behaviours and higher perceived seriousness on the consequences of engaging in those health behaviours (related to perceived severity). This, in turn, may affect their intention to perform those behaviours.

Similarly, individuals with higher level of education were found to be more concerned about the risks of computer hacking and consequences of the attacks (Grant, 2010; Zukowski & Brown, 2007); and the risks that buyers may face while doing online shopping (Chen, 2003; Sultan, Urban, Shankar, & Bart, 2003). Thus, it is expected that:

H2a: Employees with higher education level would have higher perceived susceptibility in matters related to information security.

H3a: Perceived susceptibility could mediate the direct effects of education level on employee's intention to practice information security behaviours.

H2b: Employees with higher education level would have higher perceived severity to information security incidents.

H3b: Perceived severity could mediate the direct effects of education level on employee's intention to practice information security behaviours.

On the other hand, Shaw and Spokane (2008), say that, individuals with higher education qualification would appreciate the benefits generated by engaging in physical activities more than those who are possessing low education qualifications. Literature in healthcare supports this proposition by showing that educated individuals were more likely to participate in prostate cancer screening if they perceive that, the cancer screening could produce positive returns (Gibbs, 2007). In IS literature as well, researchers comment that, farmers who are computer literate tend to value the benefits that can be generated by the usage of computers and internet in supporting their farming activities (Sharma, 2006), therefore are likely to use computers in their farming activities. Further, they show that, individuals who attained higher education level or ICT skills are more aware of the benefits of safe computing practice (Sheng et al., 2010). The positive relationship between education level and perceived benefits is also found in the following studies: Miran and Rasha, (2013); El Aziz, El Badrawy, and Hussien, (2014). Therefore, the study predicts that,

H2c: The higher the education level attained by employees, the more likely they will respond positively on the perceived benefits of information security practice.

H3c: Perceived benefits could mediate the direct effects of education level on employee's intention to practice information security behaviours.

Furthermore, education qualification can influence individual's perceived barriers to engage in some behaviour as well. For example, nurses with a lower level of academic qualifications are more likely to have a higher perception of barriers in matters pertaining to utilisation of research outputs in their daily practices (Chien et al 2013; Dean, 2004). Goldfarb and Prince, (2008) asserted that educated individuals encounter fewer barriers to internet adoption. Similarly, it is expected that individuals with higher level of education qualification may perceive lower barriers in practising acceptable information security behaviours as they have better computer skills and knowledge. In other words, the current researcher hypothesise that,

H2d: The higher the education level, the less perceived barriers in practising information security behaviours.

H3d: Perceived barriers could mediate the direct effects of education level on employee's intention to practice information security behaviours.

Perceived susceptibility refers to an individual's subjective risks of getting a disease. This perception differs widely between individuals (Orji et al., 2012).

Healthcare literature suggests that individuals with the high levels of susceptibility to disease are more likely to engage in preventive health behaviours (Rosenstock, 1966). For example, individuals are more likely to refrain from smoking because of the possibility of suffering lung cancer (McDonald et al., 2010; Reisi et al., 2014). IS literature argues that individuals with high levels of perceived susceptibility are more likely to engage in the practice of safe computing or behave more vigilantly while online (Ng et al., 2009; Siponen, Mahmood, & Pahnila, 2014). Thus, this study anticipates that,

H4: When perceived susceptibility increases, the employee's intention to practice information security behaviour increases as well and vice versa.

According to healthcare researchers, individuals would be motivated to perform the recommended health behaviours if they perceive severity of a disease could seriously affect their life (Janz & Becker, 1984; Orji et al., 2012). DiMatteo, Haskard, and Williams, (2007) and Gao et al. (2000) supported the proposition that, when a person perceives that the effect of contracting a disease could be severe, he or she would be more likely to engage in health preventive behaviour such as attending diagnosis, doing exercise and others. Similarly, IS researchers argued that if an individual perceives that the severity level of a security incident is high, that individual would be more likely to engage in practising safe computing behaviours (Jurjen Jansen & van Schaik, 2016; Lee & Larsen, 2009; Ng et al., 2009; Woon et al., 2005). Thereby, current study hypothesises that:

H5: Perceived severity could positively influence the employee's intention to practice information security behaviour.

On the other hand, healthcare researchers also suggested that an individual will intent to engage in health behaviours if the derived benefits are positively perceived (Lee, 2013; Reiser, 2007). IS researchers argued that the individual's tendency to practice information security behaviours will increase if they feel that their actions would enhance their work productivity or enjoyment (Bowen, Chew, & Hash, 2007; Escobar-Rodríguez, Carvajal-Trujillo, & Monge-Lozano, 2014;Li, Zhang, & Sarathy, 2010; Ohme, 2014; Rahman & Donahue, 2010)). Based on the literature review, this study postulates that:

H6: Perceived benefits could generate a positive effect on employees' intention to practice information security behaviour.

Previous studies asserted that individuals would be less likely to perform certain behaviours if: (1) their business rival is expected to retaliate (Lüthje and Franke, 2003); (2) they lack business knowledge and financial support and thereby may confront higher risk (Pruett et. al., 2009). In healthcare research, barriers such as perceived side effects of cancer treatment may discourage patients to seek medical consultation (Lee, 2013). IS studies indicate that perceived barriers can affect user's intention to practice security behaviours (Claar, 2011; Claar & Johnson, 2012; Ng et al., 2009) and intention to participate in online shopping for older adults (Lian & Yen, 2014). For example, Claar (2011) argued that, additional security controls in computer

systems and time constraint (such limited time to meet deadlines) may impede individual's intention to practice security behaviour. Hence, it is anticipated that:

H7: High perceived barriers would reduce employees' intention to practice information security behaviour and vice versa.

In health care study, individuals who are confident in their ability to perform a particular health behaviour would be more likely to engage in health preventive behaviours and counselling (Longo, Lent, & Brown, 1992; Rimal, 2000). For example, an individual would perform the recommended health behaviours if that individual has the confidence, skills, determination and commitment to perform that behaviour (Armitage & Conner, 2001; Floyd, Prentice-Dunn, & Rogers, 2000; Milne et al., 2000; Peyman et al., 2009; Schwarzer & Fuchs, 1996; White, Terry, & Hogg, 1994). Additionally, previous studies found that users who have information security knowledge, confidence and ability to perform certain security behaviours, are more likely to practice the information security behaviours (Claar & Johnson, 2012; Ng et al., 2009; Workman, Bommer, & Straub, 2008). The following IS literature also support this relationship (Crossler, Long, Loraas, & Trinkle, 2014; Diatmika, Irianto, & Baridwan, 2016; Nguyen & Kim, 2017; Warkentin, Johnston, Walden, & Straub, 2016). Based on the above findings, the study, hypothesise that:

H8: Self–efficacy could positively affect employee's intention to practice information security behaviours.

Cue to action is an important tool that could be used to stimulate individual's readiness to engage in appropriate health behaviour (Janz & Becker, 1984; Strecher & Rosenstock, 1997). For example, reminders letters may motivate a patient with high risks of contracting colorectal cancer to turn up for a routine check-up (Bleiker et al., 2005). In IS studies, cues to action refers to information security tips, advice, reminders, word of mouth that reminds or motivates an individual to practice information security behaviours (Claar, 2011). Great cues to action may motivate an individual to engage in protective information security behaviours (Ng et al., 2009). Therefore, the current study predicts that,

H9: Cues to action could generate positive effect on employees' intention to practice information security behaviours

The behavioural intention has widely been used as an immediate predictor of actual behaviours in social science studies (Ajzen, 1985; Webb & Sheeran, 2006). Individuals develop an intention to perform a particular behaviour before performing the actual behaviour. This implies that, actual performance of a particular behaviour is positively related to individual's behavioural intention (Conner & Armitage, 1998). Such proposition is also supported by IS literature (Al-Debei, Al-Lozi, & Papazafeiropoulou, 2013; Bradley & Prentice, 2017; Dincelli, 2017; Heirman & Walrave, 2012; Tohidinia & Mosakhani, 2010). Thus, this study hypothesises that:

H10: Intention to practice information security behaviours could positively affect the employee's actual practice of information security behaviours.

Hypothetical relationships between the constructs of the study are illustrated in figure 3.1. The additional constructs are indicated with bold circles.

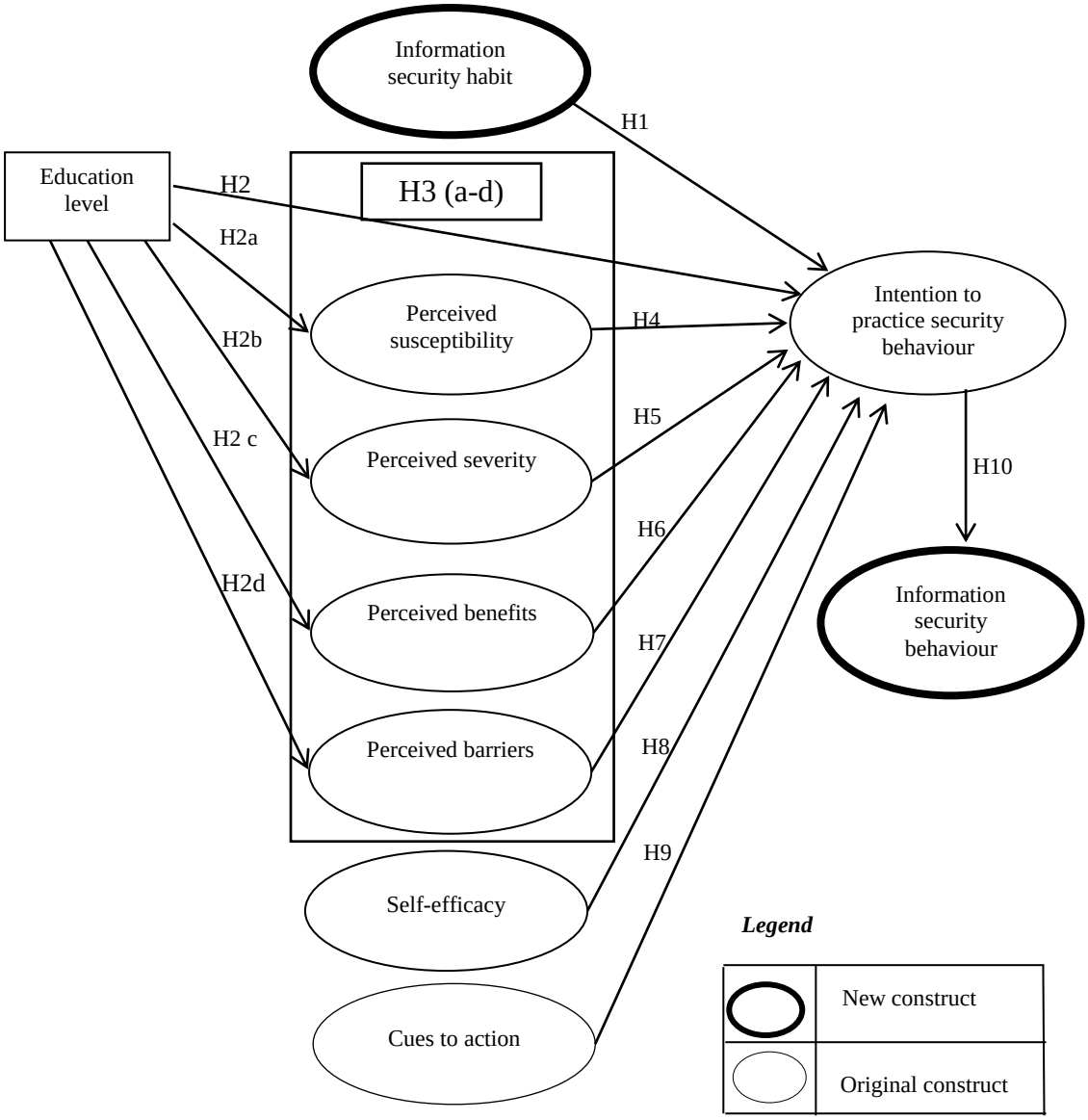


Figure 3.1: Current study's Research Model

For the sake of achieving the objectives of the study, hypothetical relationships indicated in the current research model (see figure 3.1) were examined. The first objective: was the estimation of the direct effect generated by the additional construct: information security habit, perceived susceptibility, severity, benefits, barriers, self-efficacy and cues to action on the intention of government employees on the intention to practice security behaviours was estimated by testing hypothesis H1, H4, H5, H6, H7, H8 and H9.

To measure the second objective, H2: measuring the direct effect created by the level of employees' education qualification on their intention to practice information security behaviours was tested. The third research objective is related to H2a, H3a, H2b, H3b, H2c, H3c, H2d and H3d, which involves the estimation of mediating effects caused by perceived susceptibility, severity, benefits, and barriers to the relationship between education level and intention of government employees to practice information security behaviours.

Lastly, the achievement of the fourth objective was measured by estimating the direct effect of government employees' intention to practice information security behaviours on their actual information security practice (H10). See table 3.1 for the summary of objectives and its related hypotheses.

Table 3.1: Relationships between Objectives and Hypotheses

Objective number	Relevant hypothesis or hypotheses
1	H1, H4, H5, H6, H7, H8 and H9
2	H2
3	H2a, H2b, H2c, H2d and H3(a-d)
4	H10

3.3 Research Design and Philosophy

Research paradigm is important in research due to its tremendous influence on how knowledge is studied and interpreted (Mackenzie & Knipe, 2006). It sets forth direction of the study and interpretation of the results. In social science research, the four major research paradigms: positivism, post-positivism, constructivism and critical theory are widely used.

Positivism deploys scientific methods to systematically and quantitatively generate knowledge which can be generalised from the relationships between the parameters or constructs under the study (Broom & Willis, 2007). Specifically, parameters under the study are objectively and independently manipulated by varying a single independent parameter to identify changes resulting from the inter-relationships among parameters (Henning, Van Rensburg, & Smit, 2004). Predictions are done based on the outcome or outcomes of the inter-relationships between the parameters under the study (Gicheru, 2013).

Post-positivism is not a completely new paradigm, rather an extension of positivism, which challenges how knowledge is generated in social science research (Creswell, 2012). Post-positivism argues that knowledge is not always

generated through observing and measuring parameters of the study, rather multiple perspectives (i.e. using mixed methods) should be used instead (Denzin & Lincoln, 2011; Gratton & Jones, 2010). Thus, post-positivism relies on multiple methods (mixed methods) of acquiring information such as interviews, questionnaires, observation and others.

Constructivism paradigm was developed to investigate human experience with a belief that knowledge is socially constructed (Mertens, 2005). Unlike positivism, constructivism does not start with a theory rather the development of a theory is an on-going process throughout the study and generally favours mixed method approaches of data collection and analysis (Creswell, 2013; Mackenzie & Knipe, 2006).

Whereas, critical theory is built on the premise that knowledge grows and evolves continuously through human involvement (Guba & Lincoln, 1994). Critical theory also disapproves generalisation of the results in positivism paradigm, by asserting that, the results can only be generalised if all circumstances are the same including social, political, cultural and gender (Guba & Lincoln, 1994). Critical theorists apply techniques and approaches of inquiry that foster reflection and dialogue between a researcher and a participant. The focus of inquiry is to challenge the underlying assumptions surrounding a situation under investigation (Crotty, 1998). This study uses positivism paradigm. The rationale for choosing it, is illustrated in section 3.3.1.

3.3.1 Rationale for the Choice of the Research Paradigm

Positivism was chosen based on the ground that, this study is the deductive research, which uses quantifiable measures of constructs, hypotheses are supported by the past studies' results and inferences can be drawn from findings of the current study based on level of significance (i.e. $p < 0.05$, 0.01 and 0.001) (Myers, 1997; Orlikowski & Baroudi, 1991). On top of that, the study environment including the respondent's behaviours would not be manipulated in order to reduce the chance of producing biased results. Further, using this approach, a generalisation of the findings can be achieved if the sampling method and sample size can represent the population (Easterby-Smith, Thorpe, & Jackson, 2012; Steinmetz, 2005). Details on sampling methods and sample size determination are reported in section 3.4 of this chapter.

Positivism is bound to scientific methods of investigation and quantitative approaches, in which parameters of the study can be measured, controlled and manipulated (Broom & Willis, 2007). Additionally, assumptions about the objectivity, impartiality and generalizability of the current study's results support positivism paradigm (Broom & Willis, 2007). In summary, as current study intended to objectively measure the relationship between variables and testing hypotheses (Marczyk, DeMatteo, & Festinger, 2005), positivism paradigm thereby is employed to design the study's methodology.

3.4 Sampling Design

3.4.1 Definition of Target Population

The target population of the current study is the government employees from the United Republic of Tanzania based in Dar-es-Salaam who use e-Government systems in their daily undertakings. The respondents were assumed to be computer literate with skills and knowledge to operate e-government information systems. Knowledge and skills could have been attained while in schools, learning institutions or through trainings provided by the government.

Employees of all age groups were considered as potential respondents in the study. This is because previous studies asserted that young people are believed to be comfortable with computer usage (Czaja & Sharit, 1998), while old people are more receptive and supportive towards the use of ICT (Czaja, Guerrier, Nair, & Landauer, 1993; Edwards & Engelhardt, 1989). Respondents were categorised into two age groups, 18 – 45 years and 46 years and above. This categorisation is based on the Tanzanian government employment requirements whereby lower limit for permanent and pensionable employment is 18 years and 45 years as an upper limit. For the contract and non-pensionable employees, employment age is 46 years and above. Also, these two age groups represent young and later middle or old age working groups.

The difference in levels of education was also considered when defining a target population because the literature suggests that individuals with different levels of education behave differently when using computer systems (Penard, Poussing, Mukoko, & Piaptie, 2015). Levels of education that was considered include Ordinary secondary education (O'level) to PhD level.

3.4.2 Survey Location

The study was conducted in Dar-es-Salaam, Tanzania. As the study was focusing on measuring information security behaviours of government employees', the respondents were selected from government ministries, agencies and departments (MDAs). Dar-es-Salaam city host most of the above government institutions with the comparative high use of e-government systems and ICT in general, hence an ideal study location. Besides, twenty-three (23) Authorities located in other regions (see table 3.2) currently, do not provide any online services to citizens, therefore they were not considered in this study. The total number of MDAs used in the study were 86 which is equivalent to 73% of all MDA's in Tanzania. Table 3.2 shows the distribution of the government institutions (MDAs).

Table 3.2: Distribution of Government Institutions in Tanzania (MDAs)

Category of MDA	Total Number of MDAs for each category	MDAs in Dar es Salaam Region	MDAs from Others Regions
Ministries	26	25	1
Authorities	42	19	23
Social Funds	9	9	0
Boards	17	11	6
Commissions	18	17	1
Government Companies	6	5	1
Total number	118	86	32
Percentage		73%	27%

Note: Number of MDA's were extracted from Tanzania National website in 2015

3.4.3 Sampling Technique and Procedures

The respondents were selected using the combination of proportionate stratified sampling and simple random sampling techniques from a sampling frame which is comprised of government employees with the required characteristics. Required characteristics are enumerated in section 3.4.1, page number 72. Stratified sampling was used since respondents were selected from different Ministries, Departments and Agencies (MDAs).

Firstly, the researcher identified and selected government institutions which use e-government information systems within the Ministries, Departments and Agencies (MDAs). Specifically, the researcher selected ministries, authorities, social funds, boards, commissions and government companies (see table 3.3). Secondly, to obtain respondents from each stratum (MDAs) proportionate sampling technique was used in which the number of each subgroup was determined relative to the entire population. For example, sampling composition for ministries was determined in two stages. First, the sampling composition (number of respondents from each MDA) in percentage was calculated.

$$\frac{\text{Total number of ministries}}{\text{Total number of MDAs}} = 25/86 \times 100 = 29.2\% \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (1)$$

Second, the number of respondents for the ministries was determined relative to a sample size of this study.

Sampling composition (%) x Sample size = 29.2/100 x384 = 112…….. (2)

The minimum sample size for this study was 384 respondents. Procedures used to determine the sample size are indicated in section 3.4.4. Proportional sampling is the most appropriate and common technique to select respondents from the strata (Pirzadeh, Shanian, Hamou-lhadj, & Alawneh, 2013).

Third, once the required number of respondents were established for each stratum, permission was requested from the respective MDA's (through the human resource and administration departments) to identify potential respondents. Simple random sampling was applied to select participants of the study among the identified potential respondents to ensure each participant has an equal chance of being selected. Table 3.3 shows the distribution of respondents from each MDA.

Table 3.3: Distributions of Respondents for MDAs

Category of MDA	Number of MDAs for each Category	Number of respondents from each MDA
Ministries	25	112 (29.2%)
Authorities	19	85 (22.1%)
Social Funds	9	40 (10.4%)
Boards	11	49 (12.8%)
Commissions	17	76 (19.8%)
Government Companies	5	22 (05.7%)
Total	86	384 (100%)

3.4.4 Sample Size

The targeted respondents of this study were government employees who use computer-based government information systems in their daily undertakings. To establish population size of the employees who use government information systems is difficult. Thus, Cochran's formula was used (Cochran, 1977). The formula is recommended when population size is unknown. The formula is illustrated as follows:

$$N = \frac{Z^2 P (1-P)}{d^2}$$

Where:

N: Sample size
Z: Statistic for a level of confidence (this study used Z= 1.96 since the desired level of confidence is 95%).
P: the expected proportion or standard deviation (in a proportion of one, if 50%, P = 0.5) and *d* is precision or margin error (in a proportion of one, if 5%, *d*= 0.05). A smaller *d* means good precision.

In order to calculate (sample size), the values of Z, *P* and *d* should be determined beforehand. The value for *P* can be determined based on published data of the study with similar characteristics as the current study (Naing, Than, & Rusli, 2006). With the paucity of the data and the studies of similar design and population characteristics as the current study, this study used *P* equals to 0.5 in order to yield maximum sample size for the study. The above approach is applicable when it is difficult to estimate the value of *P* (Daniel, 1999; Lwanga & Lemeshow, 1991).

Furthermore, the choice of the confidence interval (CI) for the study is subjective, randomly decided and mostly depends on the domain of the study (Aitken, Roberts, & Jackson, 2010; Rumsey, 2011). For social science studies, 95% confidence interval is used as a standard (Quirk, 2012). Thus, sample size with a confidence interval of 95% for this survey was estimated as follows:

$$N = \frac{(1.96)^2 0.5\ (1-0.5)}{(0.05)^2} = 384 \text{ employees}$$

Thus, the sample size of 384 respondents was drawn from the MDAs listed in table 3.3. The number of respondents that was drawn from each category of MDA and each MDA was determined on a proportionate basis.

3.5 Instrument and Data Collection Procedures

3.5.1 Development of the Questionnaire

This study adopted the measurement items used in the past studies to develop current study's questionnaire for data collection. The current researcher selected measurement items that were statistically significant in many past studies. On top of that, measurement items that were newly proposed by past studies were considered only if the behaviour they measure is relevant to the current study.

To avoid the repetition of items, each item was careful screened and selected. For example, an item that measures the same behaviour but had been re-worded differently in several past studies was considered as one item in the current study. This is to ensure that each measurement item is meant to measure specific and distinguished information security behaviour. Then, the questionnaire statements for each specific measurement item were developed to suit current study respondent's ability to understand and comprehend of what was measured in that statement. Academic and field experts were consulted during screening and crafting of questionnaire's statements (see section 3.5.2, page number 83 for details).

The relevant measurement items from which the pilot study questionnaire was developed are shown in table 2.3, page number 39. Selected measurement items and their respective constructs used to develop pilot study questionnaire are shown in Table 3.4.

Table 3.4: The Measurements Items for Pilot Study Questionnaire

Code	Constructs and Its Measurement Items
	Perceived Severity
PSEV 1:	If my computer is infected by malicious software such as virus as a result of opening suspicious, untrusted and unsecure websites or email attachment, my daily activities could be negatively affected [a, b].
PSEV 2:	It would cause a serious problem to me if the organisational data that is stored in my computer were stolen/ destroyed by malicious software [c, a]
PSEV 3:	I would be in trouble if my personal identifiable data such as biological traits were stolen by malicious software [d, e, f]
PSEV 4:	My personal and organisation data that are stored in my computer could be misused by cyber criminals via malicious software [d]

Table 3.4 Continue next page

Code	Constructs and Its Measurement Items
PSEV 5:	My personal and organisation data that are stored in my computer could be given to third parties without my knowledge via malicious software [d]
PSEV 6:	The invasion of malicious software could make my computer's operation become slower [d]
PSEV 7:	The invasion of malicious software could crash my computer's system from time to time[d]
PSEV 8:	The invasion of malicious software could make some of my computer programs become difficult to use [d]
	Perceived Susceptibility
PSUS1:	My computer may be infected by malicious software such as computer virus [a, i]
PSUS2:	It is possible that the cyber criminals could hack or steal the organisation data or information that is stored in my computer [b, i]
PSUS3:	The data and or application programs which are stored in and or run by my computer could be undermined or damaged by malicious software such as computer virus [j]
PSUS4:	Chances of allowing the malicious software to attack my computer could be high if I open and or use suspicious email or e-attachment [b]
	Perceived benefits
PBEN 1:	Checking whether the suspicious email/ website is NOT from a fraudulent or scammed source is an effective way to prevent malicious software from invading my computer [b]
PBEN 2:	Checking whether the file name of a suspicious website/ email/ e-attachment is NOT from a fraudulent or scammed source is an effective way to prevent malicious software from invading my computer [b].
PBEN 3:	If I can prevent malicious software from invading my computer, my work's productivity will improve [g]
	Perceived Barriers
PBAR 1:	It would be complicated for me to check whether the suspicious website or email is from trusted source [b, h]
PBAR 2:	It would be time-consuming to me to check whether the suspicious website or email is from trusted source [h, i]
PBAR 3:	To check whether the suspicious website or email is from trusted source, I may need to put in a considerable investment of some effort other than time [b, h]
PBAR 4:	It is inconvenient to me to check the source of suspected filename or web address before opening the website or emails [e, b].

Table 3.4 Continue next page

Code	Constructs and Its Measurement Items
	Cues to action
CUE 1:	If I read articles on newspaper or magazine or organisation's newsletter about computer vulnerability, I would be worried about my computer's chances of being hacked by malicious software [h, b]
CUE 2:	If I received a notice from a software developer about my computer's system security, I would be more conscious in handling my computer from being attacked [h]
CUE 3:	If a work mate have told me about his/her recent experience of the spyware, I would be more conscious in handling my computer from being attacked [h]
CUE 4:	If I receive reminders from my organisation about security attacks, I would be more cautious in handling my computer from being attacked [h, b]
	Self- Efficacy
SE 1:	I feel confident that I would be able to identify the suspicious, untrusted and unsecure websites without putting in much effort [b, h]
SE 2:	I know where and how to find the information that I need, if I encounter difficulty in identifying suspicious, untrusted and unsecure websites or emails [b, h]
SE 3:	I have the necessary knowledge and ability to protect my personal and organisation data from external threats [f, h]
SE 4:	I can identify a suspicious, untrusted and unsecure sites or email correctly without putting in much effort [f, b]
	Information Security Habits
HAB 1:	I have the habit to remove malicious software once it is detected [k]
HAB 2:	It is norm for me to check suspicious, untrusted, and unsecure websites/ emails before accessing them[e, j]
HAB 3:	It is my habit to remove malicious software periodically [j, k]
HAB4:	Checking whether a suspicious, untrusted and unsecured websites is originated from genuine source is something that I would do without being reminded to do so [e].
HAB 5:	Checking whether a suspicious, untrusted and unsecured websites or emails is not from fraudulent source is part of my daily routine [e]
HAB 6:	Checking a suspicious, untrusted and insecure websites or emails before accessing them is something that I feel weird if I do not do it [j, k]
	Intention to Practice Information Security Behaviours
BI 1:	I will actively check for suspicious, untrusted and insecure sites as a precaution before accessing them [f, k]
BI 2:	I will take precautions against information security violations [i]
BI 3:	I will never open suspicious, untrusted and unsecured sites on my computer [j]

Table 3.4 Continue next page

Code	Constructs and Its Measurement Items
BI 4:	I will continue to check for suspicious, untrusted and unsecured websites or emails that could attract my attention before accessing them.
BI 5:	I am certain that I would check for any suspicious, untrusted and unsecured websites or emails before accessing them [d, l].
	Actual Information Security Behaviours
AC1:	I check for the suspicious, untrusted and unsecured websites or emails to ensure that the websites or emails were not from fraudulent sources [d]
AC2:	Sometimes, I don't check the suspicious, untrusted and unsecured sites if it affects my performance or productivity [i]
AC3:	I check the suspicious, untrusted and unsecured websites or emails ONLY when it is convenient for me to do so[d, i]
AC4:	When I am busy, I don't check whether the suspicious websites/ emails were from fraudulent or scammed source [i]

Sources

[a] Johnston and Warkentin (2010)
[b] Ng et al. (2009)
[c] Woon et al.(2005)
[d] Liang and Xue (2010)
[e] Vance et al.(2012)
[f] Workman et al. (2008)
[h] Claar & Johnson (2012)
[I] Chan, Woon, & Kankanhalli (2005)
[j] Yoon et al. (2012)
[k] Limayem et al. (2004)
[l] Ifinedo(2012)

Likert scale was chosen as the measurement scale because the scale is easy to understand and respond to. Furthermore, with Likert scale, reliability test can easily be carried out to determine the representativeness of each item in measuring the respective variable (Baccu, 2003; Fishman & Galguera, 2003; Preston & Colman, 2000; Sullivan, 2009). In view that the current study respondents' (government employees) have a busy work schedule, hence they may be unwilling to answer the questionnaire if too many Likert scales points are used. Therefore, this study employed a five (5) points Likert scale to measure each item.

The master copy of the questionnaires was written in the English language. English and Kiswahili are official languages used by the Tanzania government institutions. Although Kiswahili is the first language, English was selected since it is used as a medium of instructions in Tanzania higher learning institutions, thus is well understood by the target respondents. Further, some of the terminologies used in this study would be difficult to understand if translated in Kiswahili. The questionnaire consisted of three parts: the first part was the cover letter; the second part was about respondent's demographic information and the third part was about the studied variable's measurement items.

The respondents were assured of anonymity and confidentiality of information collected beforehand. Specifically, respondents were informed that information collected will not be shared with any other parties and will be used for research purposes only. Also, the respondents were informed that their involvement in the study is voluntary. Appropriate measures were employed to prevent data loss and leakage of the collected data. Each respondent was required to fill in the consent form as the indication of their willingness to participate in this study. The sample consent form and ethical approval letter are attached in appendix B1, and B2, in page number 191 and page 195 respectively.

The development of current questionnaire involved two key stages: pretesting of measurement items and pilot study to test the reliability and validity of the pre-tested measurement items (Gonalves, Biscaia, Correia, & Diniz, 2014). The details are discussed in the following sub-chapters.

3.5.2 Pre-test Procedures and Results

The pre-test was done to determine whether measurement items used to measure specific information security behaviours were free from errors and can be easily understood. It helps to improve the questionnaire in the manner that prospective respondents could understand and comprehend the statements better and thereby, could respond to the questionnaire more truthfully. Therefore, in order to reduce errors and ambiguities, the questionnaire draft (see appendix B3 and B4 in page number 196 and page 204 respectively) was given to experts for verification and refinement.

The pre-test was done in two phases. In the first phase, the questionnaire was sent to the panel of five experts in the field of information systems or security to assess the clarity of words and context. The experts were selected from local universities in Tanzania, with the PhD degree in information systems or related subjects. Each expert received the letter that explains the intendment of the study, definition of each construct used in the current study and the description of each item that was used to measure specific information security behaviours. After receiving their responses, the current researcher modified the questionnaire's statements based on the experts' suggestions and preceded to the second phase. The notable changes made to the questionnaire include the inclusion of the option for government companies to accommodate government institutions that operate under the umbrella of a company or corporation such as Tanzania Telecommunication Company (TTCL) and Tanzania Railway Corporation (TRL) (see part A of the questionnaire). For

clarity and logical flow purposes, the questionnaire statement number 29 and 30 were rephrased and re-arranged, whereby the questionnaire statement number 29 was shifted to question number 30 and the vice versa. Other questionnaire statements which were rephrased include number 3, 5, 14, 27, 35, 40 and 41 (see appendix B3 and B4 for comparison).

In the second phase, the modified questionnaire was sent to another panel of five experts in the information systems or security field based in Tanzania to establish the relevancy of each item in the context of the present study. The experts were asked to rate whether each item is “not relevant”, “somewhat relevant”, “relevant” or “highly relevant”. Rating from each item was used to calculate its content validity index (CVI). CVI is the popular method in social studies for estimating content validity for the new or revised questionnaire items (Polit, Beck, & Owen, 2007).

Table 3.5 shows the CVI results. One measurement item from the construct of intention to practice information security behaviours (see item 35) was removed in the questionnaire because the index score was below the acceptable threshold of 0.78 (Polit et al., 2007). In other words, the thirty-fifth measurement item (item 35) is not the relevant item to measure intention to practice information security behaviours because it has poor content validity. As a result, 41 measurement items were used to develop the questionnaire for the pilot study, instead of 42 items.

Table 3.5: Results of Pre-test

		Ratings						
Item	Name	Expert 1	Expert 2	Expert 3	Expert 4	Expert5	Agreements	I-CVI
Item 1	PSEV1	3	3	3	4	4	5	1.00
Item 2	PSEV2	4	4	4	3	4	5	1.00
Item 3	PSEV3	4	3	3	3	3	5	1.00
Item 4	PSEV4	3	4	4	3	4	5	1.00
Item 5	PSEV5	4	4	4	3	4	5	1.00
Item 6	PSEV6	2	4	3	4	4	4	0.80
Item 7	PSEV7	4	3	3	4	4	5	1.00
Item 8	PSEV8	3	3	4	4	4	5	1.00
Item 9	PSUS1	4	3	4	3	4	5	1.00
Item 10	PSUS2	3	4	3	3	4	5	1.00
Item 11	PSUS3	4	4	3	4	4	5	1.00
Item 12	PSUS4	4	4	3	3	4	5	1.00
Item 13	PBEN1	3	1	3	4	4	4	0.80
Item 14	PBEN2	2	4	4	4	4	4	0.80
Item 15	PBEN3	2	4	4	3	4	4	0.80
Item 16	PBAR1	1	3	3	3	4	4	0.80
Item 17	PBAR2	3	3	4	4	2	4	0.80
Item 18	PBAR3	3	3	3	4	2	4	0.80
Item 19	PBAR4	3	3	3	3	2	4	0.80
Item 20	CUE1	3	3	4	3	3	5	1.00
Item 21	CUE2	3	3	2	3	4	4	0.80
Item 22	CUE3	4	4	3	3	4	5	1.00
Item 23	CUE4	3	4	4	2	4	4	0.80
Item 24	SE1	1	3	4	3	4	4	0.80
Item 25	SE2	4	4	4	3	2	4	0.80
Item 26	SE3	2	4	4	4	3	4	0.80
Item 27	SE4	2	3	3	4	3	4	0.80
Item 28	HAB1	4	3	4	3	3	5	1.00
Item 29	HAB2	2	4	4	3	3	4	0.80
Item 30	HAB3	4	4	3	3	3	5	1.00
Item 31	HAB4	4	3	3	3	3	5	1.00
Item 32	HAB5	4	4	3	4	3	5	1.00
Item 33	HAB6	3	3	4	3	3	5	1.00
Item 34	BI1	4	3	4	4	3	5	1.00
Item 35	BI2	2	4	4	2	3	3	0.60**
Item 36	BI3	4	4	4	3	3	5	1.00
Item 37	BI4	4	4	3	3	4	5	1.00
Item 38	BI5	4	3	4	3	4	5	1.00
Item 39	AC1	4	3	3	3	4	5	1.00
Item 40	AC2	3	3	4	4	4	5	1.00
Item 41	AC3	4	4	4	4	4	5	1.00
Item 42	AC4	3	3	4	4	4	5	1.00
S- CVI/Average								0.92

1- Not relevant 2- Somewhat relevant 3- Relevant 4- Highly relevant

** Deleted item

3.5.3 Pilot study Procedures and Results

The questionnaire used in the pilot study was generated after the pre-test results were statistically confirmed (see appendix B5, page number 213). A pilot study was carried out to assess validity and reliability of the data collection instrument (Baker, 1994; Dikko, 2016; Parsian & Dunning, 2009). In addition, Van Teijlingen and Hundley (2001) argue that pilot study acts as the measure of appropriateness of proposed instruments in data collection and thereby is a key determinant of whether the research project will fail or succeed.

A minimum sample size of 100 respondents is adequate in pilot study for the purpose of testing the accuracy of the measurement items reflected in the data collection instruments (Hair Jr, Black, Babin, & Anderson, 2010; Srivastava, Bhatia, Rajoura, Kumari, & Sinha, 2012; Thabane et al., 2010). The selection criteria of respondents for the pilot study were the same as the selection criteria used for selecting respondents for the main study. To elaborate, respondents of the pilot study were selected from all six participating MDA's (see table 3.6) by using stratified sampling and proportional random sampling to draw respondents from the sampling framework (see section 3.4.3, page number 74 for more details).

Table 3.6: Respondents Distribution for Pilot Study

Category of MDA	Number of MDAs for each Category	Number of respondents from each MDA
Ministries	25	29 (29%)
Authorities	19	22 (22%)
Social Funds	9	10 (10%)
Boards	11	13 (13%)
Commissions	17	20 (20%)
Government Companies	5	6 (6%)
Total	86	100

To meet the minimum sample size of 100 respondents for the pilot study (Hair Jr et al., 2010), more than 100 questionnaires were distributed. Specifically, the total of 241 questionnaires, were distributed to potential respondents. One hundred thirty-three (133) questionnaires were returned, eleven (11) were annulled as a result of the occurrence of missing data. The 122 questionnaires were therefore used in the pilot study. Demographic information of the respondents participated in the pilot study is reported in table 3.7.

Table 3.7: Demographic Information of Respondents for the Pilot Study

Demographic	Category	Frequency	Percentage (%)
Age	18 – 45	87	71.3
	46 and Above	35	28.7
Gender	Male	76	62.3
	Female	46	37.7
Education	O' Level	7	5.74
	A' Level	6	4.92
	Diploma / Equivalent	17	13.93
	Degree or Equivalent	63	51.64
	Masters	28	22.95
	Doctorate	1	0.82
Type of Organization	Ministry	35	28.69
	Authority	25	20.49
	Social Funds	11	9.02
	Boards	18	14.75
	Government Company	24	19.67

	Commission	9	7.38

3.5.3.1 Reliability Analysis for Pilot Study

Cronbach alpha was used to measure the internal reliability of the items in the questionnaire. The internal reliability test was conducted using a reliability scale module in SPSS. Table 3.8 shows that the Cronbach alpha's scores for eight (8) theorised constructs were within the acceptable range (from 0.759 to 0.898) (Biggs, Kember, & Leung, 2001; Friborg, Hjemdal, Rosenvinge, & Martinussen, 2003). Only the Cronbach alpha's score for perceived severity construct was slightly lower than other construct's scores (0.683). Nevertheless, the score is still within the range reported in other studies for the similar construct (Vance et al., 2012)**.** In summary, the responses given for each measurement item indicated that the measurement items used to measure each specific variable were reliable or consistent.

Table 3.8: Results of Pilot Items Reliability Analysis

Construct	Number of items	Cronbach alpha (α)
Perceived Severity	8	0.683
Perceived Susceptibility	4	0.862
Perceived Benefits	3	0.811
Perceived Barriers	4	0.869
Cues to action	4	0.759
Self-efficacy	4	0.839
Security Habit	6	0.898
Behaviour Intention	4	0.823
Actual Security Behaviour	4	0.784

3.5.3.2 Construct Validity Analysis for Pilot Study

Construct validity analysis was conducted through exploratory factor analysis (EFA) to determine whether the items used to measure each construct,

measures what it was supposed to measure (Peter, 1981). EFA employed maximum likelihood extraction method with Promax rotation. Maximum likelihood method was the preferred choice because it allows the estimation of a wide range of fitness indexes and permits statistical computation of factor loadings and correlations among constructs (Cudeck & O'Dell, 1994). In addition, this study uses SEM as the main data analysis technique for the hypotheses testing, which applies fitness indexes to determine how well the research data fit the model (Barrett, 2007). Thus, the use of maximum likelihood fits well with the data analysis technique employed in this study. Under Promax rotation method, it is assumed that the investigated factors are correlated because individual's behaviour is influenced by several factors that could occur simultaneously (Costello & Osborne, 2005; Cudeck & O'Dell, 1994; Fabrigar, Wegener, MacCallum, & Strahan, 1999). Kaiser Normalization was used as the criteria to decide with items to drop. The items with low reliability scores (i.e. Eigen value less than 1 and factor loading less than 0.50) were dropped (Gonalves et al., 2014; Kaiser, 1970).

EFA results (see table 3.9) show that the factor loading scores for the four measurements items of perceived severity: PSEV5, PSEV6, PSEV7, and PSEV8 are less than 0.5 and thus were removed from the study due to lack of individual reliability (Gonalves et al., 2014). In other words, items with factor loading scores equal to or greater than 0.5 were retained for the main survey.

Table 3.9: Results of Factor Analysis

Item name	PSEV	PSUS	PBEN	PBAR	CUE	SE	HAB	BI	AC
PSEV4	.716								
PSEV3	.676								
PSEV5	.689								
PSEV2	.634								
PSEV6	.410**								
PSEV8	.345**								
PSEV5	.243**								
PSEV7	.231**								
PSUS4		.656							
PSUS2		.559							
PSUS1		.531							
PSUS3		.524							
PBEN3			.723						
PBEN2			.682						
PBEN1			.646						
PBAR3				.916					
PBAR2				.807					
PBAR1				.801					
PBAR4				.667					
CUE3					.865				
CUE4					.699				
CUE2					.632				
CUE1					.512				
SE2						.948			
SE1						.821			
SE4						.712			
SE3						.698			
HAB2							.921		
HAB1							.700		
HAB4							.667		
HAB3							.517		
HAB6							.651		
HAB5							.582		
BI4								.922	
BI3								.766	
BI1								.712	
BI2								.584	
AC2									.915
AC1									.679
AC3									.564
AC4									.553

PSEV: Perceived Severity
PSUS: Perceived Susceptibility
PBEN: Perceived Benefits
PBAR: Perceived Barrier
CUE: Cues to Action
SE: Self- Efficacy
HAB: Security Habit
BI: Behaviour Intention
AC: Actual Sec. Behaviour

** Items deleted with < 0.5 factor loading

The final modified questionnaire after the completion of the pilot study, is shown in appendix B6, page number 219. This version of the questionnaire was later used to collect data in the main survey. In brief, similar to pilot study questionnaires, the main survey questionnaire was segregated into three parts, part one was the cover letter explaining the purpose and procedures for data collection and part two was meant to capture the demographic information of the respondents. In the main survey, part three consists of 37 questionnaire statements (after dropping 5 items) to examine main survey respondent's response to the studied measurement items. Their responses were then tested to measure the relationships between studied constructs.

3.5.4 Data Collection Period for Main Survey

National budget preparation is the most critical activity for MDA's. During this time, most of the Government employees are busy with annual budget preparation which usually starts from the first week of January to May. Therefore, to increase the response rate, data were collected from July to September 2016.

3.5.4.1 Questionnaire Distribution and Facilitators

Questionnaires were administered using the drop-off and pick-up approach. To ensure that, the data collection process is rigorously carried out, experienced personnel sourced from the databases of Research on Poverty Alleviation (REPOA) assisted the current researcher in the distribution of questionnaires.

REPOA is a reputable research institution based in Dar-es-Salaam, Tanzania that its main objective is to conduct research on poverty alleviation and planning policies for development.

To increase the response rate two approaches were applied. Firstly, follow–up was done on the random sample to remind the respondents who have not yet completed the questionnaires to complete them (Creswell, 2013). Secondly, trained and experienced facilitators (from REPOA) with good interpersonal relationship skills with the government employees helped in increasing the response rate and reducing the non-response rate.

3.5.4.2 Measures to Control Common Method Variance in Data Collection

Common method variance (CMV) refers to amount of inflated correlations between variables or constructs and it is likely to occur in studies that uses a single source of data, or employs a single method to collect data or applies self-reported questionnaires tool (Buckley, Cote, & Comstock, 1990; Craighead, Ketchen, Dunn, & Hult, 2011; Kemery & Dunlap, 1986). The existent of such variance could affect the final results negatively such as inflating or deflating the findings (Malhotra, Kim, & Patil, 2006; Ylitalo, 2009). The literature argues that CMV may happen due to several reasons such as social desirability, demand characteristics, consistent style in answering the questions, and ambiguity of the questionnaire statements (Ganster, Hennessey, & Luthans, 1983; Hufnagel & Conca, 1994; Podsakoff et al., 2003).

It istherefore, necessary to control the CMV effect, diagnose its presence after data collection and apply remedial strategies to minimise the effect of the variance before conducting hypothesis testing. To control the occurrence of CMV, few precautionary measures were undertaken. First, the names of the studied variables were not displayed in the questionnaire. This is to avoid the respondents to guess the relationship that should exist between the measured items of a variable. For example, the name of the variable perceived susceptibility was removed; leaving only the items which are used to measure this variable (see appendix B6, page 219). This helps to reduce the occurrence of (1) consistent answering style: giving answers without reading the statement of each measured item; (2) social desirability: providing answers to survey questions in the manner which may be favourable by others or instead of giving the answers which reflect his or her true perception (Podsakoff, Mackenzie, et al., 2003).

Secondly, anonymity and confidentiality of respondents were assured before the data collection (Li, 2015). This measure helps to reduce the respondent's evaluation anxiety issues such as fear over possible negative consequences which may arise after answering the questionnaire (Chang, Van Witteloostuijn, & Eden, 2010).

Another precautionary measure used was involving IS experts to check the questionnaire statements for ambiguous wording, demand characteristics, and relevancy of the questionnaire items to the current study (Hufnagel & Conca, 1994; Li, 2015). These procedures helped the respondents to understand and

answer each measurement smoothly. CMV diagnosis procedures and results are reported in section 4.6, page number 121.

3.5.5 Representativeness of Data to the Population

Data representativeness is important in generalising the study findings to the target population. Therefore, it is important that the study's research design is carefully planned and executed. In this study, to increase the data representativeness to the population, the following strategies were used.

The sampling error was addressed by collecting data on the site to targeted respondents. This strategy helps to reduce the possibility of selecting a sample that deviates from the targeted population's characteristics. In addition, random sampling technique was applied to ensure that every prospective respondent has a non-zero chance of participating in the study and therefore, reducing subjectivity issue (Traugutt, 2014). To reduce the non-response rate, the following-up activities were taken to remind respondents to complete the questionnaires. Research findings cannot be representative if the response rate is poor (Fincham, 2008; Holbrook, Krosnick, & Pfent, 2007).

3.5.6 Data Analysis Techniques, Tools, and Requirements

3.5.6.1 Data Analysis Techniques and Tools

Structural equation modelling (SEM) was used in this study due to its suitability to address the nature of data collected for this study. In this study, all studied variables are latent variables or each variable is measured by few items. Unlike other data analysis techniques such as multiple regressions which were frequently used in the past studies, SEM could reduce the measurement errors to occur through latent variables (variable with multiple indicators) (Liu, 1988). Measurement error refers to the extent in which the measured item deviates from its true value or ideal level of reliability and validity (DiIorio, 2005). The presence of measurement errors in the data could result in wrong interpretation of the results (Bagozzi, 1981; Schmidt & Hunter, 1996, 1999).

SEM analysis can be conducted by using two methods: covariance–based (CB-SEM) and variance–based (VB). Literature suggests that, if the study research objectives focus on testing and confirming a theory, CB-SEM based software such as *Analysis of Moment Structure* (AMOS), *Linear Structural Relations* (LISREL) and others. should be used. On the other hand, if the research focus is on the prediction and theory development, VB- SEM software such as *Smart Partial List Square* (Smart PLS), *Generalized Structured Component Analysis (GSCA)* should be used (Hair, Ringle, & Sarstedt, 2011).

Since this study tested and confirmed the extended HBM theory, thus CB-SEM based software, AMOS was used. Moreover, AMOS allows to 1) create path diagrams without launching commands; and 2) convert the validated model into a structural model for hypothesis testing, which makes the process of data analysis fast, efficient and user-friendly (Awang, 2015).

3.5.7 Missing Values Analysis

After collecting the main survey data, the missing values analysis was conducted to detect missing values. The presence of missing values may produce biased and misleading results (Pampaka, Hutcheson, & Williams, 2014). In this study, expectation–maximisation (EM) approach was used to generate a series of mean values to replace the missing values (Moon, 1996; Do & Batzoglou, 2008).

3.5.8 Data Normality Assessment and Outliers

Structural equation modelling (SEM) analysis can be used to test the studied variables structural relationship if the normality and outlier issues of data have been addressed. Only then, the SEM analysis can produce reliable results that can be generalised (Blanthorne et al., 2006; Leedy & Ormrod, 2005).

To assess the normality of current study's data, two normality tests were carried out by using AMOS data normality assessment module in which univariate and multivariate normality were examined based on the skewness

and kurtosis values. Data is considered normally distributed if the skewness absolute value is less than or equal to two and kurtosis absolute value is less or equal to seven (Curran, West, & Finch, 1996).

Data non-normality often happens in social science and psychology studies (Bentler & Chou, 1987; Bentler & Yuan, 1999). The results show that the current study data are not normally distributed, and this could affect the final results of hypotheses testing. The results of normality assessment are discussed in section 4.3.2, page 109.

The outlier is detected if the data point distance is very far from the other data points. In social and psychology studies, outliers are likely to occur due to several reasons such as respondents may have different levels of opinions or perceptions or human error may occur during data collection and data recording (Osborne & Overbay, 2008). This study analysed the presence of outliers by calculating Mahalanobis distance in AMOS software. This study indeed did detect the presence of outliers in the data set. The details of the outliers' result are reported in section 4.3.3, page number 110.

The past studies had suggested the following ways to address outliers and non-normality issues. First, to remove the outliers from the data set (Byrne, 2009) but such action may affect the structural model's results (Hair et al., 2010). Therefore, the current researcher had carried out two tests: cook's test (Cook, 1977) and Leverage test to check whether the detected outliers could affect the overall SEM results. The effect of outliers on final results is likely to occur if

cook's distance score is greater than 1.0 and Leverage's value is greater than 0.5 (Barrett, Henzi, Weingrill, Lycett, & Hill, 1999; Mauro, 1998). After conducting the above analyses, the study found that all outliers were within the acceptable range and thereby the presence of outliers will not affect the final SEM results of the study.

Alternatively, the researcher can proceed to do data analysis even though data distribution is not normal. This can be done if maximum likelihood (ML) estimation method is employed and the large sample size is used. The recommendation is supported by two reasons: 1) ML method is capable of tolerating and addressing moderate data normality violations (Bentler & Yuan, 1999; Diamantopoulos, Siguaw, & Siguaw, 2000; Graham, Hofer, & MacKinnon, 1996); and 2) The large sample sizes decrease the problem of multivariate normality (which is the case in this study) and thereby, the overall effect of non-normality distribution of current data can be considered as marginal (Hair et al., 2010; West et al., 1995). Hair et al. (2010) state that the issue of non-normality data distribution needs to be addressed if the sample size is less than 50 and its effect diminishes when sample size reaches 200. The sample size of the current study is 415.

3.5.9 Multicollinearity Tests

Multicollinearity happens when independent variables such as perceived susceptibility, perceived severity etc. are highly correlated. This is possible if (1) the correlation score between the constructs is greater than 0.80 (Awang, 2015); and (2) value inflation factors (VIF) score is greater than 10 (Marquaridt, 1970). This study conducted VIF test and confirmed the results by analysing correlation scores between the studied constructs during the analysis of the measurement model. The result shows that independent variables of the current study are not highly correlated, suggesting that multicollinearity is not present in the current research data. The details are presented in section 4.3.4 page number 111.

3.5.10 Measurement and Structural Model Validation

3.5.10.1 Construct Reliability, Validity, and Unidimensionality

The proposed research model was tested in two stages. The first stage was to test the quality of the measurement items (measurement model) through confirmatory factor analysis (CFA) and the second stage was to test the hypotheses through the structural model. The results of CFA (measurement model) were used to validate study's measurement items while results of the structural model were used to determine correlation and causal relationships between constructs (Kline, 2005). The measurement model was validated

through pooled CFA in which all constructs of the study were assessed together in a single model (Awang, 2015).

In the measurement model, construct reliability, validity, and unidimensionality must be achieved in order to ensure the measurement items are of acceptable quality. Composite reliability (CR) and Average Variance Extracted (AVE) were computed to examine the current data's reliability and validity. This study employed CR instead of Cronbach alpha to estimate the construct reliability due to the fact that CR produces accurate reliability estimates than Cronbach alpha, which has been widely used in the literature (Peterson & Kim 2013).

In measuring construct reliability, If CR value of a construct such as perceived severity is greater than 0.6, it means the measurement items used to measure perceived severity construct could reliably measure the items it is supposed to measure. On the other hand, if AVE value of a construct such as perceived severity is greater than 0.5, this indicates that the items used to measure the perceived severity construct have loaded cleanly on the construct it measures, suggesting that convergent validity has been achieved. If the square root of AVE values of constructs such as perceived severity and perceived susceptibility are higher than the scores shown in its respective row and column, this implies that these two constructs are in fact measuring different concepts, hence discriminant validity is considered achieved (Anderson, Gerbing, & Hunter, 1987; Fornell & Larcker, 1981).

On top of checking the AVE value, convergent validity can be tested by computing and analysing standardised factor loadings as well. If for example, the standardised factor loadings for each of the following measurement item: PBEN1, PBEN2, PBEN3 and PBEN4 of perceived benefits construct are statistically significance at $p < 0.05$, with t-values > 1.96, then convergent validity is considered achieved (Anderson et al., 1987).

Before running SEM analysis, current author ensured that each item used to measure constructs of the study should only measure one construct (unidimensionality) (Anderson et al., 1987). For example, the measurement items for the perceived benefit construct: PBEN1, PBEN2, PBEN3 and PBEN4 should measure only the perceived benefit construct. Unidimensionality is achieved for the perceived benefit construct when factor loadings of all measurement items (PBEN1, PBEN2, PBEN3 and PBEN4) are greater than 0.5 (Urbach & Ahlemann, 2010).

3.5.10.2 Model Fit

The series of analyses were performed to obtain the measurement model and structural model that fits well with the research data. The measures of goodness of fit were used as an indication of model fit with respect to the research data. A variety of model fit indexes were used to assess model fit. However, no set of model fit indexes can be used as an indicator of high-quality SEM results (Marsh, Hau, & Wen, 2004). Furthermore, there is no agreement on the sets of model fit indexes that should be reported in the studies involving SEM

because the performance of model fit indexes is complex to assess (Hair et al., 2010; Hu & Bentler, 1998).

Although there is no agreement was reached on determining model fit indexes that should be reported in SEM studies, the past researchers have been reporting model fit indexes from each category of model fit indexes to ensure a broad representation of each model fit indexes. Selection of model fit indexes from different categories of fit indexes has been advocated by the following researchers: Awang (2015), Hair al.,(2010), and Hu and Bentler (1998). Model fit indexes are categorised in three groups which are absolute fit, incremental fit and parsimonious fit (Awang, 2015; Hair et al., 2010).

In line with the literature's practices and recommendations, this study reported Root Mean Square Error of Approximation (RMSEA) and Comparative Fit Index (CFI) from absolute fit category, Incremental Fit Index (IFI) from category of incremental fit and relative chi-square (X^2/df) from category of parsimonious fit (see table 3.10). Category of model fit, the name of the model fit and generally acceptable cut-off values, are given in table 3.10.

Table 3.10: Model fit and Cut- off Values

Name of Category	Index	Cut- off Values	Source
Absolute model fit	RMSEA	< 0.08	Hair et al.(2010)
	CFI	> 0.90	Bentler and Bonett (1980)
Incremental model fit	IFI	> 0.90	Bollen (1989))
Parsimonious model fit	X^2/ df	< 3.00	Bentler & Bonett (1980)

3.5.11 Hypotheses Testing, Direct and Indirect Effects

Regression paths coefficients were used to assess the level of effect that an exogenous construct can predict the endogenous construct. In this study, the degree of relationship between the constructs is confirmed by the measure of statistical significance (p-values). The hypotheses are considered significant when the p-values are less than 0.05, 0.01 or 0.001 (Pedhazur & Schmelkin, 2013). Estimation of mediation effects can be achieved by using several approaches. The most common approaches are Baron and Kenny (1986), Sobel test Sobel (1982), product distribution approach (MacKinnon, Lockwood, Hoffman, West, & Sheets, 2002), and bootstrapping (Bollen & Stine, 1990; Preacher & Hayes, 2008).

The traditional approach for mediation analyses coined by Baron and Kenny (1986) has been widely criticised because of its restrictive assumption that mediation effect can only exist if the independent and dependent variables are directly related (Fritz & MacKinnon, 2007; Preacher & Hayes, 2008). In analysing the direct and indirect effects generated by education level on intention to practice information security behaviour, the current author has employed bootstrapping approach since it has higher statistical power as compared to other mediation approaches (Cheung & Lau, 2007). Bootstrapping approach reduces the chance of making type 2 error (i.e. the higher the statistical power, the lower chance of accepting a null hypothesis). Furthermore, bootstrapping allows analysis of multiple mediation effects, which suit the current study well (Paulsen, Callan, Ayoko, & Saunders, 2013).

This study involves four mediators, one independent and one dependent variable.

Multiple mediation analysis was conducted using the program called Hayes Process Macro (Hayes, 2013, 2016; Preacher & Hayes, 2008). Unlike other software, Hayes Process Macro enables simultaneous computation of multiple mediation effects, the technique which may yield better results (Paulsen et al., 2013; Preacher & Hayes, 2008). Other software such as AMOS estimates mediation effects separately, one at a time for each mediation path. The program employs bootstrapping technique which multiplies regression paths coefficients for 5,000 bootstrapping samples.

A confidence interval of 95% was set for mediators (perceived benefits, barrier, severity and susceptibility). Direct and indirect effects were assessed based on the paths coefficients, biased–corrected (BC) and confidence intervals (CI) scores. Indirect effect exists, if 95% of biased–corrected bootstrapped samples do not include zero. In other words, if zero does not occur between the lower limit confidence interval (LLCI) and the upper limit confidence interval (ULCI) of biased–corrected (BC) bootstrapped samples, indirect effect exists (Paulsen, Callan, Ayoko, & Saunders, 2013).

3.6 Summary of the Current Study' Research Methodology

Quantitative method was employed in this study. Traditional paper and pencil questionnaires were used too for data collection. The respondents were selected by using stratified sampling and proportional random sampling. The finalised measurement items for each construct were confirmed after the conduct of pre-tested and pilot test. The collected data were analysed through SEM techniques and preceded in two stages; the test of the quality of measurements and the test of study hypotheses (see chapter 4). IBM SPSS, AMOS and *Process* Macro software were used to analyse current study's data.

CHAPTER 4

FINDINGS AND DISCUSSION

4.1 Introduction

This chapter presents findings of the study and its discussion. This chapter is arranged into seven sections. The first section presents descriptive information of the respondents and its relationship with the study population. Also, it provides a brief discussion of the response rate. The second part discusses data screening procedures, data normality assessment and multicollinearity. The third section describes and presents findings of confirmatory factor analysis (CFA) and the measurement model, the fourth section discusses common method variance, and the fifth section presents results of construct validity and reliability. On the other hand, the sixth section presents the structural model and results of hypotheses, mediation effect analysis and the brief discussion of the squared multiple correlations. While, the last chapter ends with the summary of the whole chapter.

4.2 Respondent's Descriptive Information and Response rate

In the main survey, 700 questionnaires were distributed, whereby 423 were returned. This is equivalent to 60% response rate. The facilitators failed to collect the remaining questionnaires because some of the respondents were not

available in the office due to illness, leave, special assignment outside the office or the tight work schedules. Out of 423 questionnaires which were returned, 8 questionnaires were removed because the respondents did not respond to all statements concerning some variables and few pages were missing. Hence, only 415 questionnaires were used in the analysis. Nevertheless, the quantity of the collected questionnaires was sufficient for statistical analyses since it was above 384 which was the minimum amount required for this study (see section 3.4.4, page number 76 for further details).

Among the surveyed respondents, 60 % were males and 40% were females. The study's demographic profile is quite similar to the workforce distribution by gender in Tanzania public sector which reports that 59.3 % are males and 40.7% are females (NBS, 2012; URT, 2006). This finding suggests that the sample of this study is representative of the targeted population. Demographic information of the respondents for the main study is reported in table 4.1.

Table 4.1: Respondent's Demographic information for the Main Study

Demographic	Category	Frequency	Percentage (%)
Age	18 - 45	293	70.6
	46 and Above	122	29.8
Gender	Male	249	60
	Female	166	40
Education	O' Level	25	6
	A' Level	21	5.1
	Diploma / Equivalent	57	13.7
	Degree or Equivalent	208	50.1
	Masters	102	24.6
	Doctorate	2	0.5
Type of Organization	Ministry	122	29.40
	Authority	98	23.61
	Social Funds	46	11.08
	Boards	50	12.05
	Government Company	77	18.55
	Commission	22	5.30

4.3 Data Screening and Normality Assessment

It is important to perform data screening in order to conduct a successful and honest data analysis (Kim, 2010). Thus, before conducting the data analysis, data screening were performed in which missing values were checked. Thereafter, assessment of data normality, outliers and multicollinearity were conducted.

4.3.1 Missing Value Analysis Results

Missing value analysis was conducted by using missing completely at random (MCAR) approach (Little, 1988). The test was not significant (see table 4.2), indicating that there is the presence of missing values in the dataset and missing values occurred at random and without the respondent intention to skip the question. Specifically, the analysis of missing values found three (3) missing values cases. The expectation – maximisation (EM) approach with series mean method was used to replace the missing values. Missing data cases and MCAR test results are presented in table 4.2.

Table 4.2: Missing data cases and MCAR test results

Item	**Missing data ID**
PSEV 2	23
PSEV 2	58
CUE 1	121

Chi- Square Test

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	54.321a	82	0.992

4.3.2 Univariate and Multivariate Normality

From the table 4.3, the univariate normality assessment result shows that the values of skewness and kurtosis ranged from -1.1468 to -1.1838 and -1.3747 to 3.238 respectively. Although the skewness and kurtosis were within the acceptable range, this finding is not enough to conclude that current data are normally distributed (West et al., 1995). Table 4.3 also shows that the magnitude of the critical region (CR) for the few variables is greater than five (5). This finding, on the other hand, implies that current data are not normally distributed (Bentler & Wu, 2005). As both findings are contradicting, the current researcher tested the presence of outliers to confirm whether the data are normally distributed or vice versa. The results of outliers are presented in the next section 4.3.3.

Table 4.3: Univariate Normality Assessment Results

Variable	Min	Max	Skewness	C.R.	Kurtosis	C.R
Education	1	6	-1.1213	-9.3254	1.0623	4.4172
AC4	2	5	-0.4916	-4.0887	-0.0356	-0.148
AC3	1	5	-0.5783	-4.8097	1.755	7.298
AC2	2	5	-0.2591	-2.1545	-0.2279	-0.9477
AC1	2	5	-0.3042	-2.5296	-0.262	-1.0896
BI4	1	5	-0.5834	-4.852	-0.2259	-0.9394
BI3	1	5	-0.876	-7.2853	0.8984	3.736
BI2	1	5	-0.4698	-3.907	-0.0355	-0.1475
BI1	1	5	-0.7117	-5.9186	0.387	1.6094
HAB6	1	5	-0.4614	-3.8376	-0.6862	-2.8536
HAB5	1	5	-0.4377	-3.6405	-0.7787	-3.2383
HAB4	1	5	-0.7677	-6.3843	-0.4719	-1.9625
HAB3	1	5	-0.5201	-4.3256	-0.7852	-3.265
HAB2	1	5	-0.6189	-5.1468	-0.5278	-2.1946
HAB1	1	5	-0.8493	-7.0635	0.1055	0.4389
SE4	1	5	-0.1528	-1.271	-1.33	-5.5306
SE3	1	5	-0.5089	-4.2323	-0.8766	-3.6452
SE2	1	5	-0.3661	-3.0449	-0.9543	-3.9681
SE1	1	5	-0.5246	-4.3626	-0.9297	-3.8662
CUE4	1	5	-1.1468	-9.5373	1.4739	6.1289
CUE3	1	5	-1.0297	-8.5634	1.0425	4.3349
CUE2	1	5	-0.9551	-7.943	0.7275	3.0251
CUE1	1	5	-0.8909	-7.4097	-0.0005	-0.002

Variable	Min	Max	Skewness	C.R.	Kurtosis	C.R
PBAR4	1	5	0.2525	2.0998	-1.2864	-5.3494
PBAR3	1	5	0.2972	2.4717	-1.2405	-5.1584
PBAR2	1	5	0.3069	2.5526	-1.2517	-5.205
PBAR1	1	5	0.0977	0.8125	-1.3747	-5.7164
PBEN3	1	5	-0.8781	-7.3032	-0.1684	-0.7003
PBEN2	1	5	-0.5706	-4.7459	-0.679	-2.8236
PBEN1	1	5	-0.5479	-4.5567	-0.5303	-2.205
PSUS4	2	5	-0.6156	-5.1196	0.2951	1.227
PSUS3	1	5	-0.5608	-4.6644	1.3456	5.5956
PSUS2	1	5	1.1838	9.8449	3.238	13.4645
PSUS1	1	5	-0.5808	-4.8302	0.5812	2.4168
PSEV4	1	5	-0.8578	-7.1343	-0.1131	-0.4705
PSEV3	1	5	-0.5402	-4.4926	-0.7591	-3.1565
PSEV2	1	5	-0.9184	-7.6381	-0.2547	-1.059
PSEV1	1	5	-0.5932	-4.9333	-0.7514	-3.1246
Multivariate					113.3026	20.9313

4.3.3 Multivariate Outliers

Assessment of outliers was conducted by calculating mahanolobis distance: the distance from the centroid (Byrne, 2009). The first twelve (12) observations were of the concern in this study since they showed much deviation from the centroid, with p values < 0.001 (Kline, 2005) (see appendix C, page number 224). The percentage of outliers was 2.9% (12/415).

Although outliers and multivariate non-normality were detected, the study continued with further statistical analyses without removing or transforming the research data to become normally distributed. This is because the presence of outliers and multivariate non-normality may not necessarily affect the final results. The following statistical results and the literature support this proposition.

1) Cook's distance and leverage score results are within the acceptable range: 0.00031 to 0.01914 and 0.02493 to 0.03483 respectively, thus the final results will not be affected (see appendix D, page number 226).

2) Multivariate non-normality has no effect because the sample size of this study is large enough to suppress the effect of multivariate normality.

3) The study conducted by Reinartz, Haenlein and Henseler (2009) found that there is no difference in final results of SEM studies which employed maximum likelihood estimation (MLE) on the sample data with different levels of kurtosis and skewness.

The detailed discussion on the data normality has been presented in section 3.5.8, page number 96 of this thesis.

4.3.4 Correlation Estimates and Multicollinearity Results

The correlation estimates of each pair of the constructs indicate that the relationship between the pairs is not strong (see appendix E, page number 230) and this implies the absence of multicollinearity problem. However, this evidence is not considered a conclusive indication that multicollinearity problem does not exist (Naser, Karbhari, & Mokhtar, 2004). Therefore, the additional test which checks on value inflation factor (VIF) for each construct

was carried out to check whether multicollinearity between constructs does exist. From table 4.4, the results show that the VIF values are within the acceptable range: of less than 10 and this further confirm that the studied variables are not highly correlated.

Table 4.4: Variance Inflation Factor Results

Constructs	Coefficients	T-Ratio	Significance level	VIF Values
Severity	-.053	-1.025	.306	1.140
Susceptibility	.066	1.302	.194	1.085
Benefit	-.004	-.072	.943	1.261
Barrier	.000	.000	1.000	1.131
Cues	-.087	-1.741	.082	1.069
Self-Efficacy	-.037	-.553	.581	1.880
Habit	-.051	-.794	.428	1.746
Intention	.200	3.610	.000	1.305

4.4 Confirmatory Factor Analysis Results

CFA involves latent variables, thereby education level was not included in CFA because this variable is the categorical variable (Awang, 2015). Based on the recommended threshold values (refer table 3.10, page number 102), the current measurement model (CFA model) did not produce satisfactory results to meet model fit cut-off values. Basically, the results indicate that while absolute fit and the parsimonious fit was achieved by measurement model, the incremental fit was not achieved.

As the incremental fit indices (IFI and CFI) did not meet the minimum cut-off values (see Table 4.5), the initial measurement model (shown in figure 4.1) was modified several times by deleting items with low factor loading (i.e.

below 0.5) in each round, until all model fit indices achieved the minimum cut-off values.

Table 4.5: Model Fit Results for Initial Measurement Model

Model fit	Name of Index	Value	Comment
Absolute model fit	RAMSEA	0.053	Acceptable level achieved
Incremental model fit	IFI	0.884	Acceptable level not achieved
Incremental model fit	CFI	0.883	Acceptable level not achieved
Parsimonious model fit	X^2/df	2.019	Acceptable level achieved

In summary, items that were deleted due to low factor loadings were, PSEV2, CUE1, SE3, HAB4 and PSUS2. These items were used to measure the following variables: cues to action, perceived severity, perceived susceptibility, self-efficacy, and the security habit respectively .Figures for the modified measurement models are reported in the appendix, F, G H and I in page number 231, 232, 233 and 234 respectively. The factor loading score for each item after omission of the items with low factor loading score is shown in table 4.6.

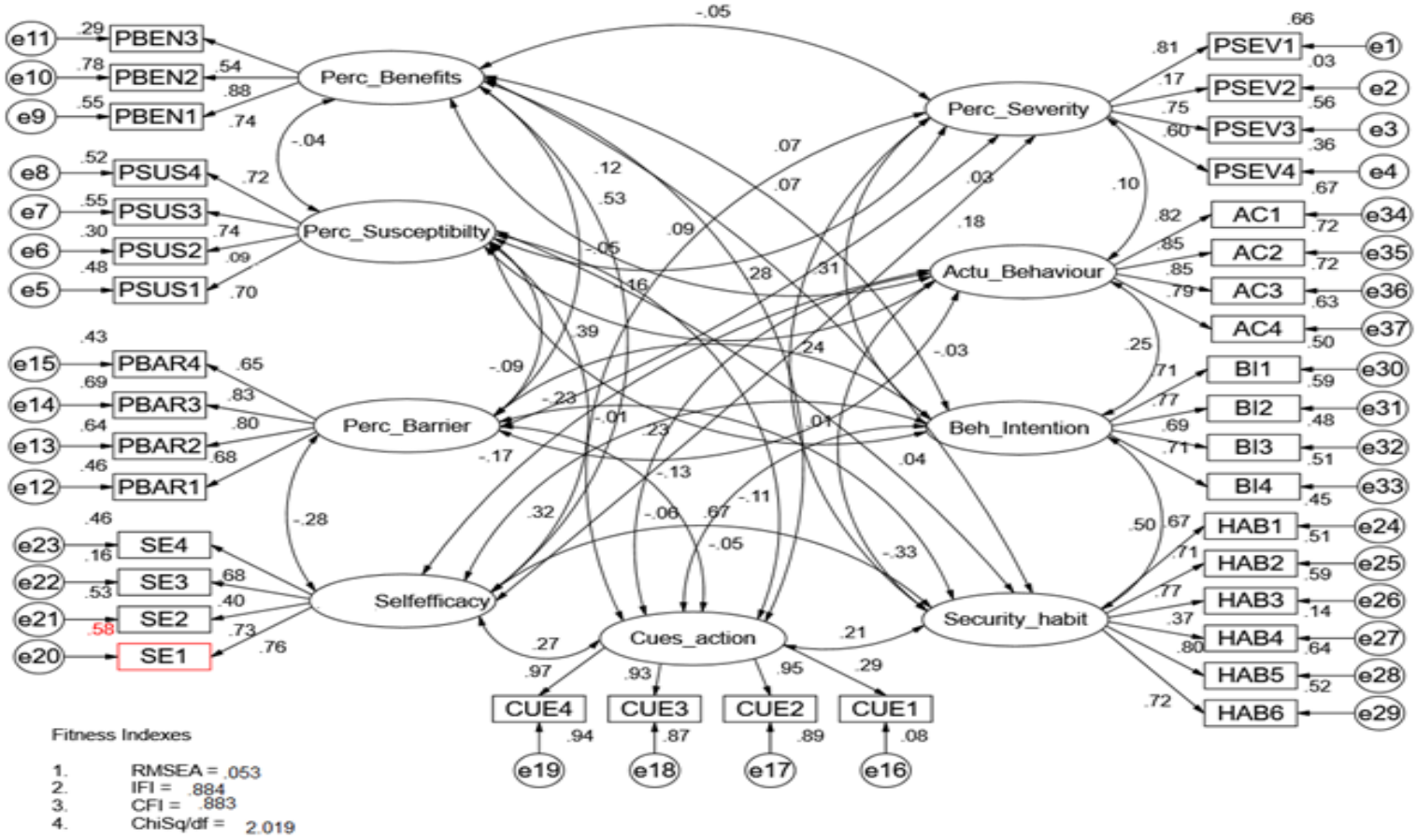


Figure4.1: Initial Measurement Model

Table 4.6: Item Factor Loadings

Construct	Item	Factor loading
Perceived Severity	PSEV1	0.81
	PSEV2	Deleted**
	PSEV3	0.75
	PSEV4	0.60
Perceived Susceptibility	PSUS1	0.67
	PSUS2	Deleted**
	PSUS3	0.75
	PSUS4	0.75
Perceived Benefits	PBEN1	0.74
	PBEN2	0.88
	PBEN3	0.54
Perceived Barrier	PBAR1	0.68
	PBAR2	0.80
	PBAR3	0.83
	PBAR4	0.65
Cues to action	CUE1	Deleted**
	CUE2	0.95
	CUE3	0.93
	CUE4	0.97
Self- efficacy	SE1	0.76
	SE2	0.72
	SE3	Deleted**
	SE4	0.68
Security habit	HAB1	0.67
	HAB2	0.71
	HAB3	0.77
	HAB4	Deleted**
	HAB5	0.81
	HAB6	0.72
Behaviour intention	BI1	0.71
	BI2	0.77
	BI3	0.69
	BI4	0.71
Security behaviour	AC1	0.82
	AC2	0.85
	AC3	0.85
	AC4	0.79

** Items deleted with < 0.5 factor loading

The final measurement model that was obtained after modification of the initial measurement model, produced acceptable model fit values. This finding confirms the factorial validity of the measurement model of the study. Model fit results for the final measurement model are reported in table 4.7. The final measurement model is shown in figure 4.2.

Table 4.7: Model fit results for the final measurement model

Model fit	Name of Index	Value	Comment
Absolute model fit	RAMSEA	0.043	Acceptable level achieved
Incremental model fit	IFI	0.950	Acceptable level achieved
Incremental model fit	CFI	0.949	Acceptable level achieved
Parsimonious model fit	X2/df	1.773	Acceptable level achieved

4.5 Validity, Reliability and Unidimensionality

After confirming the factorial validity of the measurement model, convergent validity, discriminant validity and unidimensionality were analysed. The findings show that average value extracted (AVE) scores were above the acceptable threshold of 0.5 (see table 4.8), which implies that convergent validity is achieved (Fornell & Larcker, 1981). This means all measurement items that are supposed to measure each construct are truly related to each other. For example, items PBAR1, PBAR2 and PBAR3 used to measure the construct of perceived barriers are related.

Next, discriminant validity was assessed to ensure that items used to measure one construct are different from other items or could be discriminated from another construct's items. The study found, that the square root of AVE was higher than scores in its rows and columns (see bolded diagonal values in table 4.8), therefore discriminant validity was achieved**.** This means, the measurement items used to measure for example the construct of perceived barriers is different from the measurement items used to measure other constructs of the study, therefore measurement items used in this study measured different concepts.

Table 4.8: Inter-item Correlations CR and AVE Score for each Construct

	CR	AVE	PSEV	PBEN	HAB	PSUS	PBAR	SE	AC	BI	CUE
PSEV	0.765	0.525	**0.724**								
PBEN	0.773	0.541	-0.030	**0.735**							
HAB	0.857	0.546	0.236	0.106	**0.739**						
PSUS	0.766	0.523	0.263	-0.035	0.037	**0.723**					
PBAR	0.831	0.553	0.032	-0.055	-0.322	-0.081	**0.744**				
SE	0.765	0.521	0.173	0.524	0.666	-0.033	-0.285	**0.722**			
AC	0.896	0.682	0.094	-0.162	0.004	0.369	-0.027	-0.189	**0.826**		
BI	0.812	0.520	0.311	0.074	0.504	0.217	-0.228	0.318	0.249	**0.721**	
CUE	0.964	0.898	-0.069	-0.088	-0.210	0.131	0.126	-0.279	0.056	0.047	**0.948**

PSEV: Perceived Severity
PBEN: Perceived Benefits
AC: Actual Security behaviour
CR: Composite Reliability
HAB: Security habit
PSUS: Perceived susceptibility
BI: Behaviour intention
AVE: Average Variance Extracted
PBAR: Perceived Barrier
SE: Self-efficacy
CUE: Cues to action

Table 4.9 also supports the convergent validity results, whereby factor loadings for each standardised measurement item is statistically significance at the level $p< 0.001$.

Figure 4.9: Standardised Item Factor Loadings

Item	Standard Error	Critical Ratio(t- Values)	P-Values
PSEV 1	0.0 87	6.675	***
PSEV3	0.084	8.435	***
PSEV4	0.075	12.216	***
PSUS1	0.027	10.946	***
PSUS3	0.021	8.975	***
PSUS4	0.028	9.087	***
PBEN1	0.06	9.459	***
PBEN2	0.079	4.431	***
PBEN3	0.078	13.177	***
PBAR1	0.089	12.15	***
PBAR2	0.074	9.565	***
PBAR3	0.069	8.447	***
PBAR4	0.089	12.405	***
CUE2	0.047	9.658	***
CUE3	0.045	7.416	***
CUE4	0.039	10.479	***
SE1	0.072	9.967	***
SE2	0.071	10.971	***
SE4	0.093	11.7	***
HAB1	0.054	13.065	***
HAB2	0.061	13.025	***
HAB3	0.055	11.765	***
HAB5	0.048	8.82	***
HAB6	0.052	11.16	***
BI1	0.037	11.248	***
BI2	0.032	9.793	***
BI3	0.037	11.545	***
BI4	0.04	11.335	***
AC1	0.029	11.296	***
AC2	0.022	11.403	***
AC3	0.019	9.153	***
AC4	0.031	11.675	***

Table 4.9 Continue next page

Item	Standard Error	Critical Ratio(t- Values)	P-Values
Note:			
PSEV: Perceived Severity		HAB: Security habit	PBAR: Perceived Barrier
PBEN: Perceived Benefits		PSUS: Perceived susceptibility	SE: Self-efficacy
AC: Actual Security behaviour		BI: Behaviour intention	CUE: Cues to action
Significant at *** p <0.001			

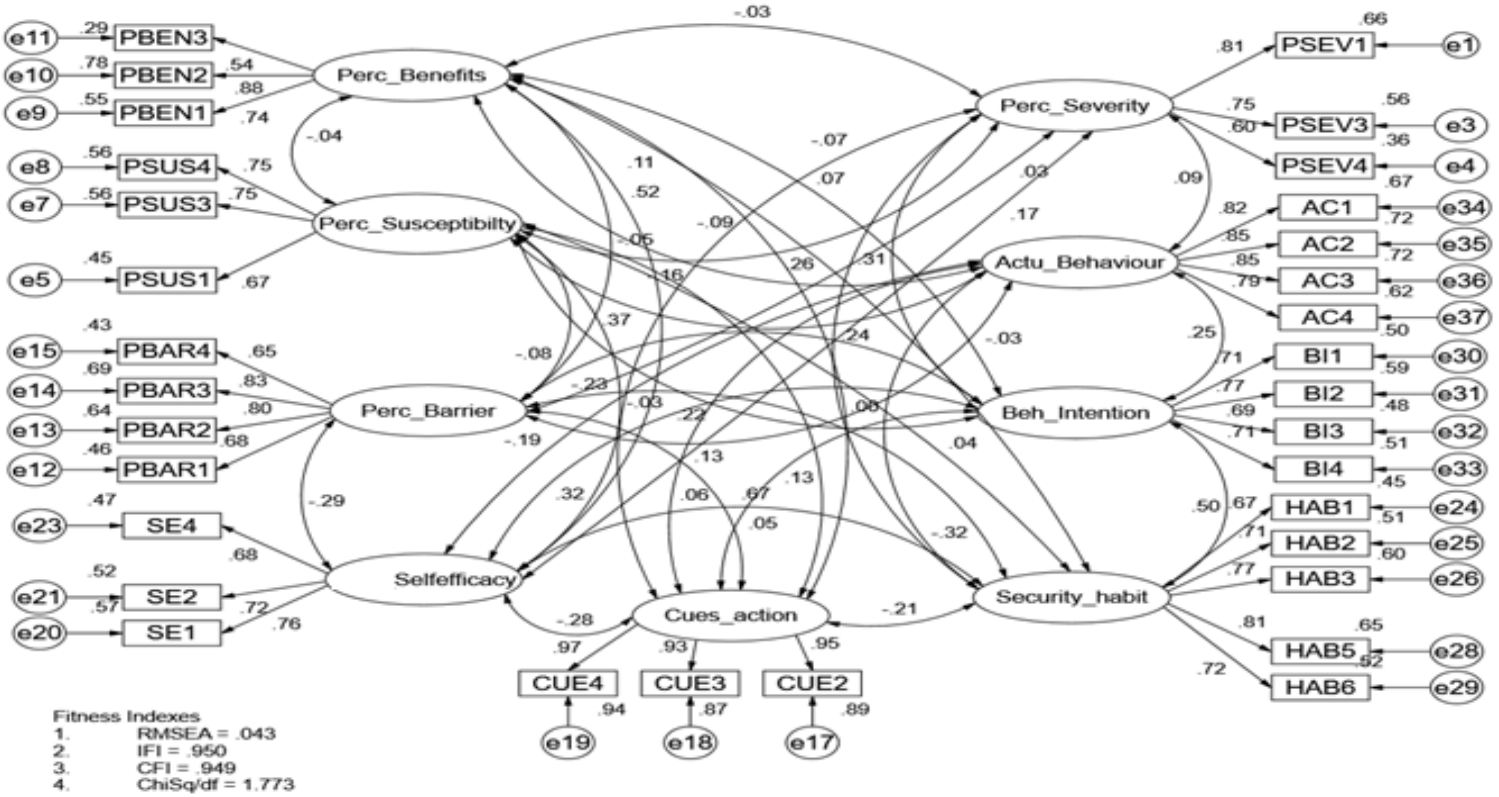


Figure 4.2 : Final Measurement Model

With regard to unidimensionality, the study found that factor loadings for all measurement items were above 0.5 (see figure 4.2) and therefore unidimensionality has also been achieved. To elaborate, the measurement items (such as PBAR1, PBAR2 and PBAR3) which were used to measure perceived barriers construct are in fact measuring only the perceived barriers construct, and not any other construct.

The reliability of the items was assessed by examining the CR values. From table 4.8, it is noted that all CR values are above the acceptable threshold or above 0.6. Based on the CR values, the measurement items of each construct (such as measurement items of perceived barriers construct: PBAR1, PBAR2 and PBAR3) are reliable measures of the perceived barriers construct. In addition, in order to compare responses on the scale of 1 to 5 (whereby 1= strongly disagree, 5= strongly agree), the mean scores for each construct was computed. Mean score for each construct is reported in table 4.10.

Table 4.10: Construct Mean scores

Code	Name	Mean Score
PSUS	Perceived susceptibility	3.73
PSEV	Perceived severity	4.51
PBEN	Perceived benefits	3.37
PBAR	Perceived barriers	4.71
CUE	Cues to action	4.62
SE	Self-efficacy	2.78
HAB	Security habit	4.86
BI	Behaviour intention	4.72

Note:

PSEV: Perceived Severity	HAB: Security habit	PBAR: Perceived Barrier
PBEN: Perceived Benefits	PSUS: Perceived susceptibility	SE: Self-efficacy
BI: Behaviour intention	CUE: Cues to action	

4.6 Common Method Variance Results

Although the following precautionary measures were taken to control CMV during data collection – such as removing names of the studied variables in the questionnaire; ensuring respondents could comprehend the questionnaire's statements by removing ambiguous wordings; and assuring the respondents of anonymity and confidentiality of the collected data, Harman's single factor and common latent factor tests were carried out (Chang et al., 2010) to detect the presence of CMV. This is because the study used a self-administered questionnaire that may introduce common method variance on the collected data (Campbell, 1982).

Harman's single factor test was conducted by using IBM AMOS software, in which all items of the study were represented as indicators of a single factor. The study found that the resulting model did not fit with the research data and this shows that CMV is not the serious issue in this study (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003; Podsakoff & Organ, 1986). The diagram for Harman's single factor test is reported in appendix J, page 235. The results of Harman's single factor test are reported in table 4.11.

Table 4.11: Harman's Single Factor Test Results

Model fit	Name of Index	Value	Comment
Absolute model fit	RAMSEA	0.169	Acceptable level not achieved
Incremental model fit	IFI	0.105	Acceptable level not achieved
Incremental model fit	CFI	0.105	Acceptable level not achieved
Parsimonious model fit	X^2/df	12.811	Acceptable level not achieved

To confirm the results of Harman's single factor test, common latent factor analysis (CLF) was conducted (Williams & Anderson, 1994). In examining the CLF results, the standard regression weights for each measurement item were compared. Table 4.12 shows that the difference in standardised regression weights between the items of the study before and after the conduct of CLF test was less than 0.2. This indicates that CMV is not serious (Gaskin, 2012). In other words, the estimation of hypothetical relationships (H1, H2, H3 etc.) in current study's structural model is unlikely to be affected by CMV (i.e. there is no systematic error variance from the collected data which may cause correlations between studied constructs to deviate from the true population values).

Table 4.12 : Common Latent Factor Test Results

Items	Paths	Construct	Std. regression weights (with CLF)	Std. regression weights (without CLF)	Difference in regression weights
PSEV1	<--	Perc_Severity	0.8083	0.8127	0.0044
PSEV3	<--	Perc_Severity	0.7511	0.7565	0.0054
PSEV4	<--	Perc_Severity	0.5965	0.5967	0.0002
PSUS1	<--	Perc_Susceptibilty	0.6745	0.6751	0.0006
PSUS3	<--	Perc_Susceptibilty	0.7472	0.7475	0.0003
PSUS4	<--	Perc_Susceptibilty	0.7446	0.7466	0.002
PBEN1	<--	Perc_Benefits	0.7418	0.7421	0.0003
PBEN2	<--	Perc_Benefits	0.8826	0.8828	0.0002
PBEN3	<--	Perc_Benefits	0.5301	0.5399	0.0098
PBAR1	<--	Perc_Barrier	0.6785	0.6788	0.0003
PBAR2	<--	Perc_Barrier	0.796	0.7976	0.0016
PBAR3	<--	Perc_Barrier	0.831	0.8344	0.0034
PBAR4	<--	Perc_Barrier	0.645	0.6547	0.0097
CUE3	<--	Cues_action	0.7909	0.9309	0.14
SE1	<--	Selfefficacy	0.7579	0.767	0.0091
SE2	<--	Selfefficacy	0.7218	0.7242	0.0024
SE4	<--	Selfefficacy	0.6746	0.6834	0.0088
HAB1	<--	Security_habit	0.667	0.6676	0.0006
HAB2	<--	Security_habit	0.7122	0.7139	0.0017
HAB3	<--	Security_habit	0.7716	0.7725	0.0009
HAB5	<--	Security_habit	0.807	0.809	0.002
HAB6	<--	Security_habit	0.7231	0.724	0.0009
BI1	<--	Beh_Intention	0.7078	0.7095	0.0017
BI2	<--	Beh_Intention	0.7688	0.769	0.0002

Items	Paths	Construct	Std. regression weights (with CLF)	Std. regression weights (without CLF)	Difference in regression weights
BI3	<--	Beh_Intention	0.6925	0.6927	0.0002
BI4	<--	Beh_Intention	0.7112	0.7116	0.0004
AC1	<--	Actu_Behaviour	0.8201	0.8204	0.0003
AC2	<--	Actu_Behaviour	0.8374	0.8461	0.0087
AC3	<--	Actu_Behaviour	0.8444	0.8467	0.0023
AC4	<--	Actu_Behaviour	0.7892	0.7905	0.0013
CUE4	<--	Cues_action	0.6657	0.75012	0.08442
CUE2	<--	Cues_action	0.6712	0.79546	0.12426

Note:

PSEV: Perceived Severity	HAB: Security habit	PBAR: Perceived Barrier
PBEN: Perceived Benefits	PSUS: Perceived susceptibility	SE: Self-efficacy
BI: Behaviour intention	CUE: Cues to action	AC: Actual Security Behaviour

4.7 Structural Model Results

Specification of the structural model and hypotheses testing were conducted next. During structural model specification, the final measurement model (see figure 4.2, page number 119) was transformed into the initial structural model (see figure 4.3, page number 126). The transformation of the measurement model into the structural model was guided by the underlying current conceptual framework of this study (see figure 3.1, page number 67). The full structural model consisted of all constructs (latent variables) found in the final measurement model with the additionally observed variable, which is education level.

The past studies suggest that categorical variables (such as education level) with two to four sub-categories and continuous variables (such as perceived barriers) should be treated differently in SEM studies if maximum likelihood (ML) estimation technique is used (Innami & Koizumi, 2013; Johnson & Creech, 1984; Rhemtulla, Brosseau-Liard, & Savalei, 2012). Treating

categorical data with less than four sub- categories as continuous data may produce distorted results due to the generation of biased estimates, incorrect standard errors and model fit indices (Rhemtulla et al., 2012). In this study, categorical variable (education level) was treated in a similar manner with continuous data since it consists of more than five sub-categories (O'level, A'level, Diploma or Equivalent, Degree or Equivalent, Master's Degree and PhD) (see table 4.1, page 107), therefore the final structural model results may not be distorted.

Also, residuals were added to all endogenous variables and covariance was established between exogenous variables (Awang, 2015). The residuals are used to accounts for all variance on endogenous variables that were not included as antecedent variables of it and covariance was established between exogenous variables because all exogenous variables share some variance between them (O'Rourke & Hatcher, 2013). Using maximum likelihood estimation (MLE), the structural model yielded the model fit indices as indicated in table 4.13.

Table 4.13: Model Fit Results for Initial Structural Model

Model fit	Name of Index	Value	Comment
Absolute model fit	RAMSEA	0.050	Acceptable level achieved
Incremental model fit	IFI	0.900	Acceptable level not achieved
Incremental model fit	CFI	0.899	Acceptable level not achieved
Parsimonious model fit	X^2/df	2.046	Acceptable level achieved

Figure 4.3 shows that the current study's model fit indices for the initial structural model were not satisfactorily achieved because some model fit indices failed to achieve the required level (refer table 3.10, page number 102

for the acceptable model fit indices). Thereby, the current researcher had modified the structural model to improve the model fit indices. The modification of the initial structural model followed the similar procedures that were employed during modification of the measurement model. The initial structural model is shown in figure 4.3.

.

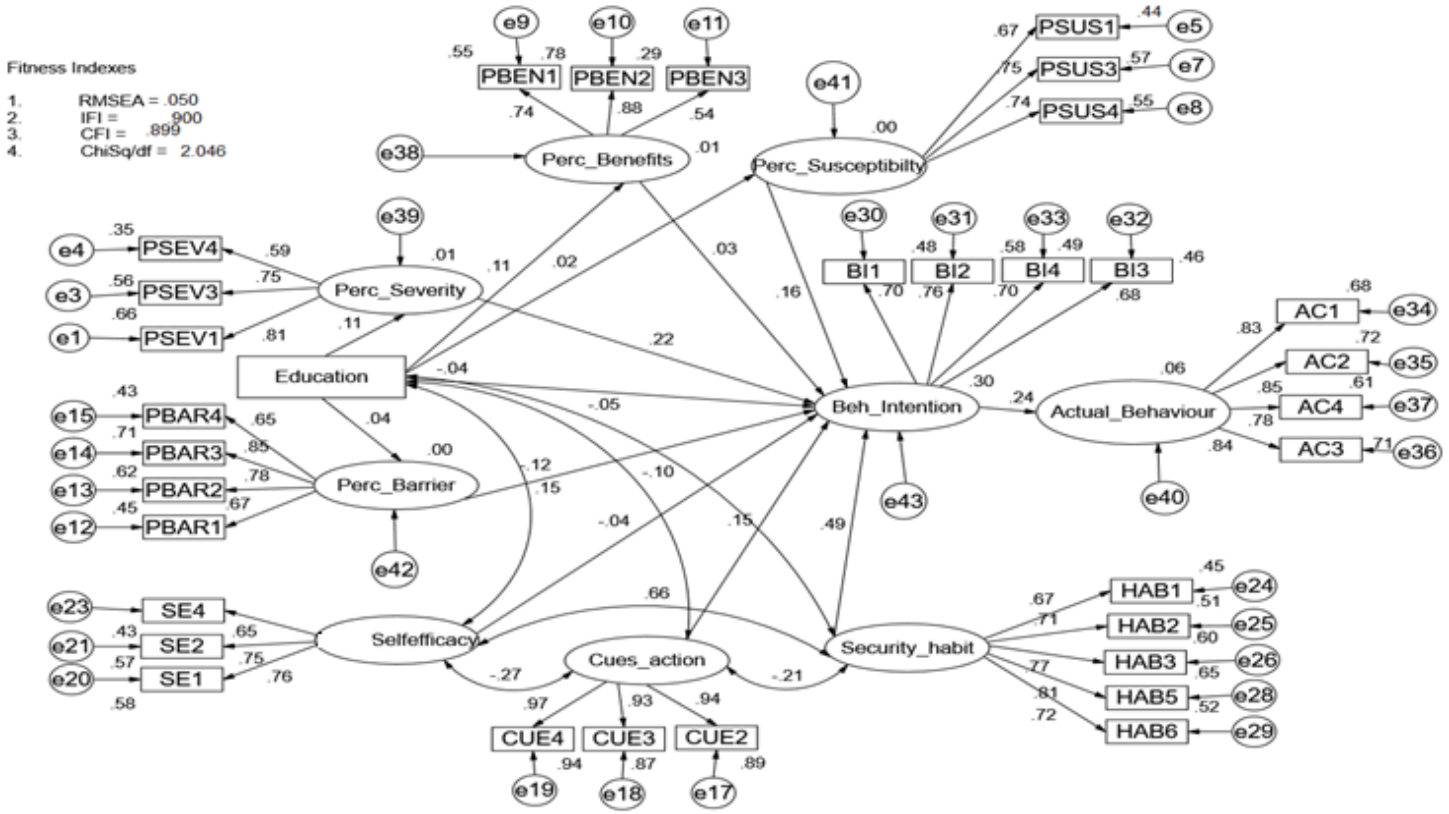


Figure 4.3: Initial Structural Model

Parameter scores in the modification indices showed items HAB 1(e24) and HAB 2 (e25) (see table 4.14) would largely improve model fit if it will be set free (constrained) as compared to other items enlisted in the modification indices (see table 4.14). After setting HAB 1 and HAB 2 as free parameters, model fit improved as shown in table 4.14.

Table4.14: Modification Indices Scores

Items/ Paths	Modification Index	Expected Change
e40 <--> e41	29.5408	.0973
e36 <--> e37	25.4216	.0514
e34 <--> e35	18.6449	.0457
e28 <--> e29	33.2431	.1994
e25 <--> e29	18.9644	-.1610
e24 <--> e25	40.5023	.2230

The results of model fit (see table 4.15) show that the data used in this study have finally fitted well in the structural model. The final structural model is shown in figure 4.4.

Table 4.15: Model Fit Results for Final Structural Model

Model fit	Name of Index	Value	Comment
Absolute model fit	RAMSEA	0.053	Acceptable level achieved
Incremental model fit	IFI	0.917	Acceptable level achieved
Incremental model fit	CFI	0.916	Acceptable level achieved
Parsimonious model fit	X^2/df	2.160	Acceptable level achieved

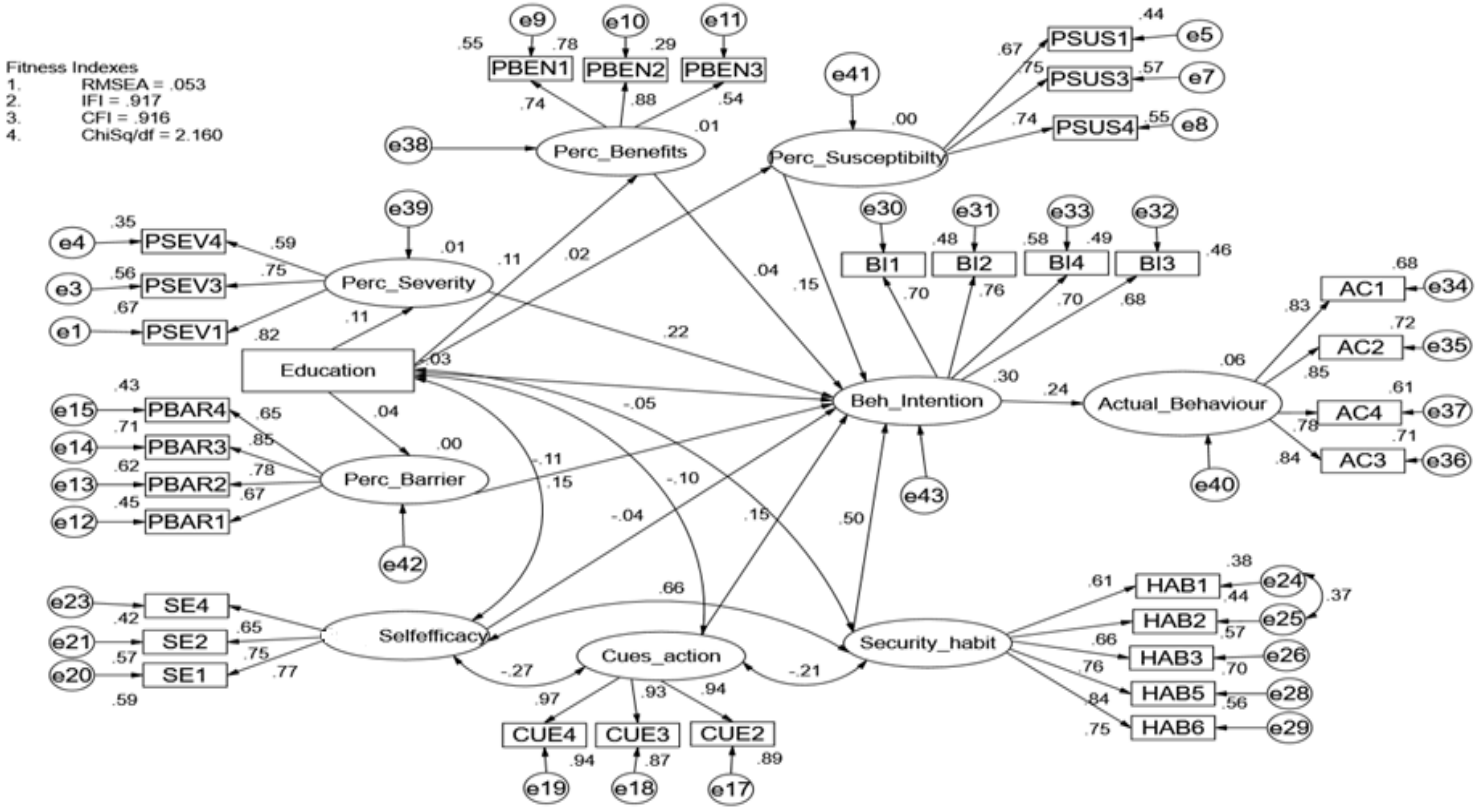


Figure 4.4: Final Structural Model

4.8 Hypotheses Testing Results

The hypotheses were tested based on the regression paths coefficients of the final structural model at 0.05, 0.01 and 0.001 significance levels. From table 4.16, eight (8) the hypotheses are supported while five (5) hypotheses are not supported. The findings of this study are presented in reference to research objectives of the study.

Table 4.16: Hypotheses and Regression Paths Coefficients

Constructs		Constructs	Estimate	C.R.	P-Value	Comments
Security Habit	→	Intention (H1)	0.477	5.278	***	Supported
Education	→	Intention (H2)	-0.020	0.654	0.513	Not Supported
Education	→	Susceptibility (H2a)	0.011	0.41	0.682	Not Supported
Education	→	Severity (H2b)	0.109	2.002	0.045*	Supported
Education	→	Benefits (H2c)	0.084	1.978	0.048*	Supported
Education	→	Barriers (H2d)	0.035	0.734	0.463	Not Supported
Susceptibility	→	Intention (H4)	0.195	2.664	0.008**	Supported
Severity	→	Intention (H5)	0.130	3.768	***	Supported
Benefits	→	Intention (H6)	0.027	0.659	0.510	Not Supported
Barriers	→	Intention (H7)	-0.075	-2.136	0.033**	Supported
Self-efficacy	→	Intention (H8)	-0.026	0.468	0.64	Not Supported
Cues to action	→	Intention (H9)	0.122	2.89	0.004**	Supported
Intention	→	Security behaviour (H10)	0.240	4.059	***	Supported

Note: Significant at *p < 0.05, **p<0.01, ***p<0.001

4.8.1 Direct Effects of Studied Variables on Intention to Practice Information Security

This section is meant to address the first, second and fourth research objectives. Specifically, in this section results on the relationships between the perceptions of: susceptibility, severity, benefits, barriers, cues to action, self-efficacy and information security habit on employees' intention to practice information security; are compared with the past studies' results. Also, plausible explanations for the findings are discussed.

The following hypotheses were tested: H1, H2, H4, H5, H6, H7, H8, H9 and H10 to address the research objectives.

To address the research, the first research objectives, hypotheses H1, H4 to H9 were tested. The study found that; if the government employees exercise information security habits, their intention to practice information security behaviours would increase. This finding supports H1 (see Table 4.16). The statistical significance of information security habits on behaviour intention to practice information security behaviours is consistent with the previous IS studies (Jia & Hall, 2014; Pahnila et al., 2007a). This finding is also supported by the mean score of 4.86 (which is the highest mean score as compared to mean scores of the other constructs) (see table 4.10), indicating that, most of the respondents strongly agree than disagree, that the habit of checking for suspicious, untrusted and unsecure websites before accessing them, (see table 3.4, page number 78 for the measurement items of information security behaviours) could increase their intention to execute information security behaviours. This belief could have eventually made this construct the significant predictor of intention to practice information security behaviours.

Table 4.16 shows that perceived susceptibility creates a positive significant effect on intention to practice information security behaviours, therefore H4 is supported. This finding is consistent with the previous studies conducted by Crossler (2010), LaRose and Rifon (2007), Liang and Xue (2010) and Siponen et al. (2014). H5 which predicted that perceived severity would have a positive influence on intention to practice information security behaviours is supported

as well. This finding suggests that, if the respondents perceive that information security attacks on information systems may lead to the serious problems, then they would have been more likely to practice the information security behaviours. This finding is consistent with the previous studies conducted by Chenoweth, Minch, and Gattiker, (2009), Lee, LaRose, and Rifon, (2008), and Jansen and Schaik (2016).

The plausible explanation for the statistical significance of H4 (perceived susceptibility) and H5 (perceived severity) could be due to the prevalence of information security attacks that had been experienced by Tanzania's private and government institutions (Citizen, 2014; Nfuka, Sanga, & Mshangi, 2014). For example, Mwananchi (2016) reported ATM fraud worth of over 10 billion TZS (equivalent to 5 million USD) was stolen between the year 2010 and 2013. In addition, Mutarubukwa (2010) and Amir (2016) reported information security attacks to government information systems, whereby several government websites were taken down by the hackers and important information was stolen.

Such kind of experience may have increased Tanzania government employees' perceived susceptibility level (i.e. government information systems are also prone to information security attacks) and perceived severity level (i.e. information security attacks may cause severe loss) to practice information security behaviours.

H6, which predicted that perceived benefits could have a positive influence on the intention to practice information security behaviours, is not supported. The observation on the mean score result of perceived benefits construct shows that, most of the respondents had the neutral perception (reflected by the mean score equivalent to 3.37 see table 4.10, page number120) on the benefits of practising information security behaviour. Mean score of this construct suggests that, perceived benefits to practice of information security behaviours could be important to the respondents, but if they do not know how to harness those benefits, they may become less interested in reacting neither positively nor negatively. As a result, the perceived benefits of practising information security behaviour could not lead the government employees to the motivation of practicing information security behaviours. Non-significant influence of perceived benefits on intention to practice information security behaviours corroborates with the previous IS studies which found the similar result. (Claar, 2011; Horst, Kuttschreuter, & Gutteling, 2007).

This study support H7. To elaborate on the effect of perceived barriers on intention to practice information security behaviours, it is important to review the items that have been used to measure this variable in this study (see table 3.4, page number 78 for the measurement items of perceived barriers). In relation to the measurement items used to measure this construct, perhaps tasks that involve checking for suspicious email or websites are complicated, time, consuming, or tedious for the respondents. The presence of the above possible barriers could have in turn reduced their intention to practice acceptable information security behaviours. The above explanations are also supported by

the mean score of this construct. This construct had the mean score of 4.71 (see table 4.10, page number 120), which suggests that most of the respondents agree rather than disagree to perceived barriers items in the questionnaire. This finding is consistent with Bourg's (2014) study, who also found that perceived barriers have negative influence on intention to practice information security behaviours.

In this study, the respondents' self- efficacy in information security may not influence their intention to practice information security behaviours (denoted by H8). Using the same approach taken to discuss the effects of perceived benefits and perceived barriers, it is necessary to understand why respondents' self-efficacy could not influence their behavioural intention towards information security behaviours.

From the questionnaire (see appendix B6), respondents were requested to judge their own self-efficacy: confidence, knowledge, and ability to identify suspicious websites or malicious software. Construct mean score results (see table 4.10, page number 120) indicates that the mean score for the self-efficacy construct is 2.78, which can be labelled as low. The literature suggests that individuals with low self-efficacy have the tendency to avoid tasks which do not match with the level of skills they possess (Ede, Hwang, & Feltz, 2011). Previous studies also argue that Tanzania government employees lack information security skills due to inadequate provision of information security trainings and relevant information security education in the academic syllabus (Dewa & Zlotnikova, 2014;Bakari et al., 2005; Nungu, 2012; Tarimo et al.,

2006). Thus, plausible reasons for non- significant results on the relationship between self-efficacy and intention to practice information security behaviour could be due to low self-efficacy and lack of information security skills. This finding is consistent with the previous IS studies (Tamjidyamcholo, Baba, Tamjid, & Gholipour, 2013; Youn, 2009; Wall, Palvia, & Lowry, 2013).

As predicted, cues to actions such as the use of news articles, notice from software developer, reminders from the organisation management and word of advice from the work mates, could significantly increase the intention of the government employees to practice information security behaviours, indicating that H9 is supported .Possibly, the presence of the alerts on the possibility of the occurrence of information security incidences issued by Institution's ICT departments or word of mouth between work mates could have increased government employees intention to practice information security behaviours. The finding is consistent to study carried out by Jenkins, Durcikova, and Burns's (2011). Nevertheless, the finding is inconsistent to study conducted by Ng et al. (2009). Possibly, Ng et al.'s (2009) study's respondents were IT savvy, and thereby the use of cues to actions was not helpful to persuade them to practice information security behaviours anymore.

The second research question was addressed by the testing hypothesis H2. The finding indicates that education level did not produce the significant direct effect on government employees' intention to practice information security behaviours, suggesting that H2 is not supported. The plausible reasons for this finding could be the knowledge of practising information security is not well

articulated in the academic syllabus of computing and non-computing programmes in learning institutions (Nungu, 2012). Therefore under-emphasis of information security education and training in higher learning institutions in Tanzania could have tremendously affected government employees' information security behaviours. It should be noted that majority of the respondents had acquired higher education (refer to demographic information of respondents in table 4.1, page number 107). Furthermore, the government employees are not given adequate training pertaining on how to handle the security of the information (Bakari et al., 2005; Dewa & Zlotnikova, 2014; Tarimo, Bakari, Yngström, & Kowalski, 2006; Tarimo et al., 2006). In other words, even though some of the respondents were highly educated, they were less knowledgeable on basic information security practices.

With regard to the last research objective, the actual practice of information security is strongly influenced by the intention of the government employees to practice information security behaviours or H10 is supported. This finding suggests that when government employees' intention to practice information security increases, their actual behaviour in practising the information security behaviour would increase as well. This finding corroborates with the past IS studies carried out by Eccles et al., (2006), Ajzen and Fishbein, (2005), Liang and Xue, (2010), Webb, (2006), and Yoon et al. (2012).

4.8.2 Mediation Effects of Susceptibility, Severity, Barriers, Benefits on Intention to Practice Information Security

To address the third research question, firstly, the direct effect caused by education level on the following variables: perceived susceptibility, severity, benefits and barriers represented by hypotheses H2a, H2b, H2c, and H2d respectively were tested. Secondly, mediation effects were analysed to test the hypotheses H3 (a-d).

Table 4.16 shows that the effects of respondents' education level on perceived severity of information security attacks (H2b) and respondents' education level on perceived benefits of exercising information security behaviour respectively (H2c), are statistically significant. The finding with regard to H2b is consistent with Chen (2003) and Sultan, Urban, Shankar and Bart (2003) findings, while the finding with regard to H2c is consistent with El Aziz, El Badrawy and Hussien (2014) studies. Possible explanation for this finding could be effect of basic computer skills attained by the employees while in learning institutions (majority of higher learning institutions provide the course on introduction to computers which is usually taught to all students). Hence, computer skills attained could have helped government employees to understand benefits and consequences of an information security attack (severity or seriousness of the attacks). On the other hand, the effects generated by education level on perceived susceptibility (H2a) and perceived barriers (H2d) were statistically non-significant. Possible explanation for this finding can be as follows:

Information security skills are different from ordinary or basic computer literacy skills, such that an individual may display good computer skills but may fall short of information security skills and security awareness (Maumbe & Owei, 2012). To elaborate, an individual needs to possess some basic information security skills to identify possible susceptible and malicious online resources (Davinson & Sillence, 2010). In other words, the basic computer skills acquired by those who were educated in higher learning institutions could have helped them to understand the information security benefits and severity of security attacks, but the skills were not sufficient to enable them to detect susceptible online resources and to overcome the barriers of practising information security behaviours. In summary, lack of information security skills could decrease the Tanzanian government employees' perceived susceptibility to information security attacks and increased perceived barriers to practice information security behaviours.

The findings with regard to H2a and H2d are inconsistent with the following IS research studies carried out by Chen, (2003), Davinson and Sillence, (2010), Sheng, et al., (2010), and Sheng et al., (2007). The inconsistency in findings could be caused by the nature of the respondents. Contrary to this study, respondents in the above mentioned past studies were trained to practice acceptable information security behaviours. Therefore, the information security training provided could have improved the past studies respondents' perceived susceptibility and reduced perceived barriers on intention to practice information security behaviours.

Further analysis was conducted to address the third research question by examining the mediation effects. To analyse mediation effects of perceived severity, susceptibility, benefits and barriers on intention to practice information security, education level was treated as an exogenous variable. Meanwhile, perceived benefits, barriers, severity and susceptibility served as mediators and intention to practice information security served as endogenous variable.

To compute the total effect generated by the education level on employees' intention to practice information security, few steps were involved .First, the direct effects of education level without involving mediators were examined by calculating the effect of education level (exogenous variable) on intention to practice information security (endogenous variable). The study found that the path between education level and intention to practice information security behaviour was not significant (see table 4.17). Second, the direct effect of education level on intention to practice information security behaviour was examined by including the effects created by the mediators (see table 4.17).

Table 4.17: Direct Effects of Education Level on Intention to Practice Information Security

Construct	Effect type	Estimated effect	BC-LLCI	BC-ULCI	Results
Education level	Direct effect (Without mediators)	-0.03100	-0.0975	0.0356	Not significant
Education level	Direct effect(With mediators)	-0.05670	-0.1221	0.0087	Not significant

BC-LLCI= Bias-Corrected Lower Limit Confidence Interval BC-ULCI= Bias-Corrected Upper Limit Confidence Interval

The results from the computation of total and direct effect of education level on intention to practice information security indicate that, there is no direct effect of education level on intention to practice information security before and after the introduction of mediators. This finding suggests that education level has no direct relationship with intention of the government employees to practice information security behaviours, thus, the only potential relationship between education level and intention to practice information security behaviour could be through the mediators. Furthermore, the slight decrease on the estimated effects (from -0.03100 to -0.0567) after the introduction of mediators apparently confirms the assertion that education level could likely produce an indirect effect (through mediators) rather than the direct effect in the current study.

This finding is inconsistent with the previous IS studies (Sheng et al., 2007; Sheng et al., 2010). Possible explanation for the difference in the finding between the current study and the above mentioned previous IS studies could be information security training that was given to respondents in previous studies during the study. For example, in the study conducted by Sheng et al. (2010) the intention of the respondents to avoid phishing emails trap improved sharply after receiving information security training.

Third, the indirect effects of education levels (with mediators) on the intention of Tanzania government employees to practice information security behaviours were estimated (see table 4.18). Among the four mediators, the effect of education level through perceived severity on employees' behavioural intention

was found statistically significant. In other words, perceived severity does mediate the effects of education level on the intention of Tanzania government to practice information security behaviours (H3b). This finding suggests that education level could have increased government employees' perceived severity levels to information security attacks, which in turn increased their intention to practice information security behaviours.

Table 4.18: Indirect Effects of Education Level on Intention to Practice Information Security Behaviour

Construct					Estimated effect	BC-LLCI	BC-ULCI	Results
H3a: Education	→	Susceptibility	→	Intention	0.00180	-0.0068	0.0146	Not Significant
H3b: Education	→	Severity	→	Intention	0.02470	0.0102	0.0451	Significant
H3c: Education	→	Benefits	→	Intention	0.00220	-0.0069	0.0157	Not Significant
H3d: Education	→	Barriers	→	Intention	-0.00300	-0.0170	0.0081	Not Significant

BC-LLCI= Bias-Corrected Lower Limit Confidence Interval

BC-ULCI= Bias-Corrected Upper Limit Confidence Interval

The study also found that the mediation effects through perceived susceptibility (H3a), perceived benefits (H3c) and perceived barrier (H3d) on the intention of Tanzanian government employees to practice information security behaviours were non-significant (see table 4.18). The previous studies have indicated that information security education or training may produce substantial improvement in the user perceptions on intention to practice information security behaviours (Bulgurcu, Cavusoglu, & Benbasat, 2010; Davinson & Sillence, 2010;Thomson & von Solms,1998). Hence, plausible reasons for this finding could be the inadequate or lack of information security training and lack of education to Tanzania government employees besides formal education attained in higher learning institutions.

4.9 Squared Multiple Correlations (R^2)

Squared multiple correlations (R^2) indicates how much the exogenous constructs have explained the dependent variable (Schumacker & Lomax, 2015). Each endogenous construct has its own R^2 which indicates the amount of variance explained by each construct in the model (see table 4.19).

Table 4.19: Squared Multiple Correlations for Endogenous Construct

Construct	R^2
Perceived Susceptibility	.0005
Perceived Severity	.0122
Perceived Barrier	.0015
Perceived Benefits	.0114
Behaviour Intention	.3008
Actual Security. Behaviour	.0559

Computation of the overall R^2_min this study employed the formula coined by Pedhazur (1982) as follows:

$$R^2_m = 1- (1- R^2_1) (1- R^2_2) \ldots (1- R^2_n).$$

Where: R^2_m is Overall Squared Multiple correlations
R^2 is squared multiple correlations for each individual construct
1- R^2 is the unexplained variance for each regression equation.

Therefore, the overall R^2 is calculated as:

= 1 – (1- 0. 0015) (1-0.0114) (1-0.0005) (1-0.0122) (1-0.3008) (1- 0.0559)

= 0.38

The overall multiple squared correlations (R^2_m) denotes that 38% of the variance in the dependent variable is explained by the structural model. For the squared multiple correlations (R^2_m) to adequately explain the dependent

variable should be not less than 10% (Cohen, 1988; Falk & Miller, 1992). This study achieved $R^2_m = 0.38$ which is well above the range**.** Thus, the overall multiple squared correlations (R^2_m) obtained in this study is adequate to explain the dependent variable.

4.10 Summary

This chapter presented and discussed empirical data findings of the study including results of missing values analysis, data normality, outliers, common method variance, construct validity, reliability and unidimensionality, measurement model (CFA model), common variance method, structural model, hypotheses testing and direct and indirect effects. The discussion of each finding has also been provided. AMOS, SPSS and *Hayes Process* macro were used for data analysis. A number of tests were conducted to check missing values, data normality and multicollinearity to ensure that data meet the requirements of SEM analyses. Most of the requirements were met except for data normality.

The research utilised recommendations from the literature to address the data normality issue. The measurement model and structural model achieved cut-off values of model fit indices indicating factorial and structural validity of the models. The study found that eight (8) out of thirteen (13) direct hypotheses were supported.

Further, findings from the mediation analysis indicated that perceived severity mediates the relationship between education level and the intention of government employees to practice information security behaviours.

CHAPTER 5

CONCLUSION

5.1 Introduction

This chapter comprises of five sections. The first section provides an account of the accomplishment of the research objectives. The second section presents theoretical implications. The third section presents policy implications based on statistical results of the study. The fourth section presents limitations of the study and the last section provides direction for the future research.

5.2 Accomplishment of Research Objectives

To address the research problem, this study accomplished four objectives, which are first, evaluation of the direct effects generated by the perceptions of susceptibility, severity, benefits, barriers, self-efficacy, cues and the practice of security habit on government employees' intention to practice information security behaviours. Second; examination of the direct effects created by employees' level of' education qualification on their intention to practice information security behaviours. Third, estimation of the mediation effects of susceptibility, severity, benefits, and barriers on the relationship between education level and government employees' intention to practice information security behaviours. Fourth, to evaluate the direct effects of employees'

intention to practice information security behaviours on their actual information security practice.

To accomplish the first objective, the employees' perceptions: information security habits, susceptibility, severity and cues to action, tested by hypotheses H1, H4, H5 and H9 respectively, were found to have positive influence on the intention of Tanzania government employees to practice information security behaviours, while perceived barriers tested by hypothesis H7 had negative influence. On the other hand, benefits of practising information security behaviours and self-efficacy tested by hypotheses H6 and H8 respectively indicate that could not influence Tanzania government employees' intention to practice information security behaviours.

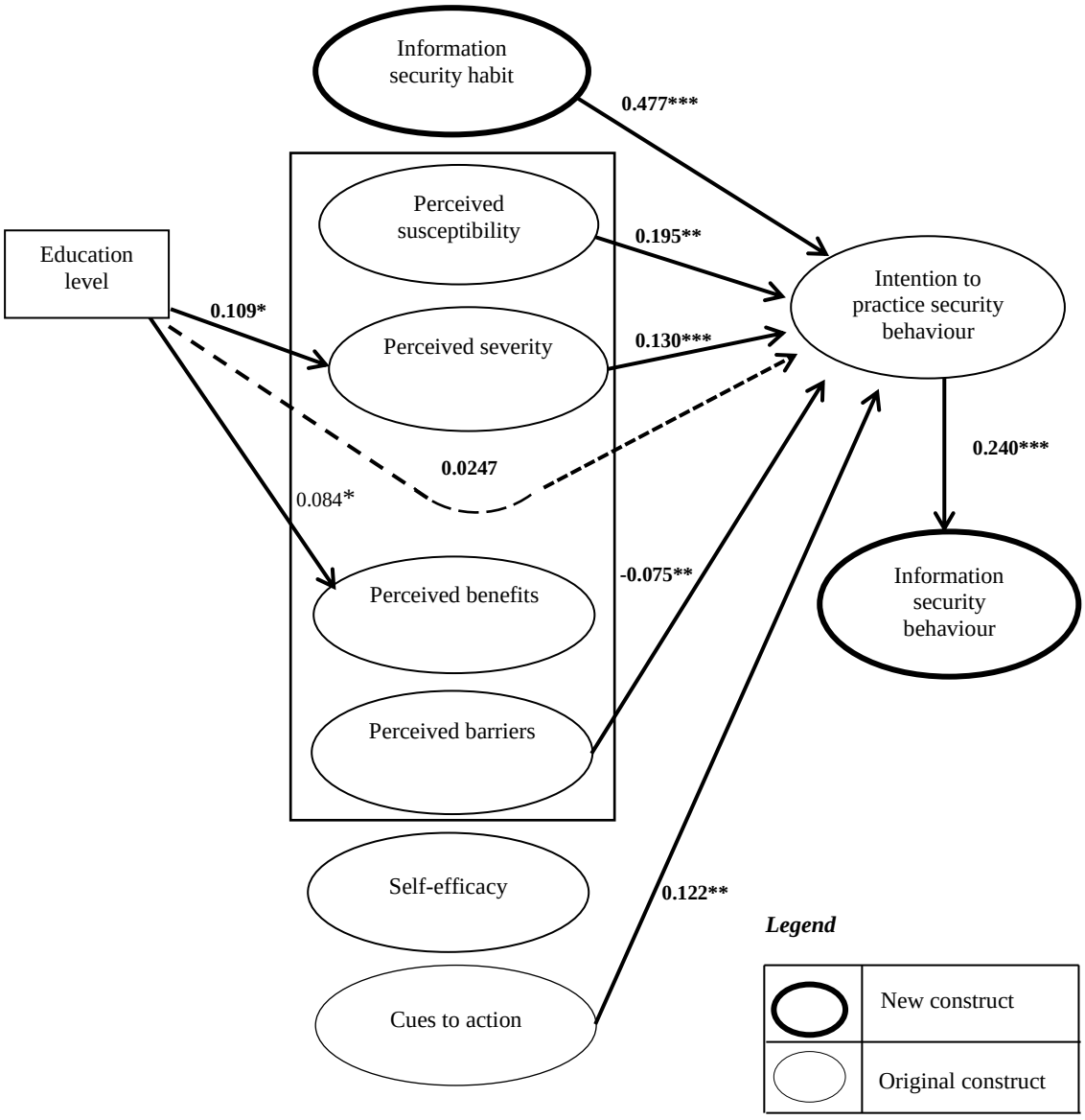
With regard to the second objective, the study found that similar to H6 and H8, the level of education qualification achieved by the government employees (tested by hypotheses H2) could not influence the Tanzania government employees' intention to practice information security behaviours. The third objective was achieved by estimating mediation effects of perceived susceptibility, severity, benefits, barriers on intention to practice information security behaviours tested by hypotheses H2a, H2b, H2c, H2d and H3(a-d). The study found that that the level of education qualification attained by Tanzania government employees could not impact their perceptions with regard to susceptibility to security attacks (H2a) and barriers to practice information acceptable security behaviours (H2d) directly.

On the other hand, the level of education qualification could directly influence employees' perceived severity levels on information security attacks (H2b) and perceived benefits of practising information security behaviours (H2c). Indirectly effects of education level on perceived susceptibility (H3a), perceived benefits (H3c) and perceived barriers (H3d) could not influence the intention of the employees to practice information security behaviours. However, indirect effects of education level through perceived severity construct (H3b) could influence the intention of the government employees to practice information security. This finding indicates that the effects of employees' education level on intention to practice information security behaviours could only be mediated by the perceived severity construct.

The fourth objective was accomplished by testing H10. The study found that the increase intention of the government employees to practice information security could lead employees to practice information security when using e-government information systems.

In conclusion, the outcomes of this thesis can be utilised by information security practitioners, policy and decision makers as the base for enhancing information security behaviours of information systems users for effective management and cultivation of information security in Organisations. The final research model is shown in figure 5.1.Standard estimate values have been indicated to the significant relationships only. Also significant relationships are indicated by bold arrow lines. The results for mediation analysis (significant mediation effects of perceived severity construct on the relationship between

education level and intention to practice information security behaviours) are indicated by dashed lines. Additional constructs are indicated with bold circles.



Note: Significant at *p <0.05, **p<0.01, *** p<0.001

Figure 5.1: Final Research Framework with Standard Estimates

5.3 Theoretical Implications

A number of theoretical implications to academics can be deduced from the findings of this study. Firstly, the significant impact of information security habits in predicting the intention to practice information security behaviours provides two insights.

1) The extant literature in information security behaviours such as Boss, Kirsch, Angermeier, Shingler, & Boss, 2009; Chan et al., 2005; Claar, 2011; Claar & Johnson, 2012; Dinev, 2008; Hanus & Wu, 2016; Liang & Xue, 2009;. Ng et al., 2009; Pahnila et al., 2007; Pahnila, Siponen, & Mahmood, 2007; Workman et al., 2008) focused more on the influence of conscious related constructs on information security behaviours. The findings of this study enrich the extant literature on information security behaviours by examining the effects generated by both conscious and non-conscious security behaviours variables. In this way, the relatively and more comprehensive theoretical framework to better understand human information security behaviours, has been developed. This theoretical framework refines further our understanding on how both conscious and non-conscious behaviours integrate into shaping employees' intention to practice information security behaviours. Notably, our findings indicated that security habits (non-conscious behaviour) had higher significant effect in motivating an individual to practice information security behaviours as compared to conscious behaviours.

2) The scarcity of studies in information security behaviours that examine the effect of information security habits has created the knowledge gap in understanding of information security behaviours. The findings of this study, particularly on significant effects of security habit on intention to practice information security behaviour is an attempt to addresses this knowledge gap. Further, significance influence of the security habits addresses the weakness of the original HBM to measure habitual behaviours (Taylor et al., 2007) and validates the extension of the original model, thus the research model developed can be used to study habitual behaviours as well.

Secondly, the significant influence of intention to practice information security behaviours on actual information security behaviour in this study validates further, the extension of the original HBM. Moreover, due to the fact that behavioural intention does not always lead to the actual practice of behaviours (Herath, 2013); future studies may use the extended model to study actual information security behaviours as a dependent variable instead of behavioural intention.

Thirdly, while the role played by cognitive perception variables (susceptibility, severity, benefits and barriers) in mediating the effect of education level on intention to perform behaviours is common in other fields of study (for example health care field), such mediation relationships have been rarely tested in the study context of information security. The significant mediation effects

of perceived severity on the relationship between education level and intention to practice information security behaviour found in this study, further refine our knowledge on how the construct of perceived severity could impact the intention to practice information security behaviours. Specifically, this finding informs researchers that, apart from directly influencing the intention to practice information security behaviour this construct also mediates the relationship between education level and intention. Further, this finding could serve as the step forward for the future studies to further investigate the mediation effect caused by perceived severity on the relationship between other demographic factors (such as age, income, ethnicity) and intention to practice information security behaviours

5.4 Policy Implications

Based on the findings, this study provides a number of implications for policy and decision makers in organisations as a guide to enhance information security behaviours of their employees.

This study found that employees' intention to practice information security behaviours is positively related to their perceptions of severity and susceptibility to security attacks. Therefore, policy and decision makers should strive to maintain higher levels of perceived severity and perceived susceptibility among the government employees. This can be achieved through information security training, education programs and information security awareness campaigns. This suggestion is in line with the previous studies

which found that, the use of training, education programs and participation in awareness campaigns in both health care and IS research fields, caused significant increase in perceptions of severity and susceptibility among the targeted respondents, which ultimately increased their likelihood to perform the recommended behaviours (Hanus & Wu 2016; Davinson & Sillence, 2010; Ahlan et al., 2015; Hochbaum, 1958; Rosenstock, 1966).

In addition, this thesis recommends the use of incentives or rewards and punishments or sanctions to maintain higher levels of perceived severity and susceptibility. According to Straub (1990), incentives or rewards may motivate a person to practice good information security behaviours and vice versa for the impact of punishment. For example, employees who reported suspicious internet activities and use strong passwords could be rewarded while, employees who use suspicious and untrusted websites could be punished or sanctioned (Paulsen & Coulson, 2011).

As cues could significantly influence the employees' intention to practice information security behaviours, tools such as pop-up message could be displayed when an employee is accessing websites or online resources. This will serve as the reminder for the users to practice acceptable information security behaviours (Johnston & Warkentin, 2010). Other cues such as reminders notices and information security newsletters could also be helpful for increasing information security awareness among government employees (Dowland, Furnell, Illingworth, & Reynolds, 1999; Khan, Alghathbar, & Khan, 2011), enhance information security knowledge, create the facilitative

environmental context that stimulates the intention to practice security behaviours and influencing user's devotion towards information security behaviours (Michie et al., 2005).

Cues can be disseminated physically to employees, in the forms of newsletters, posters, memo or through institutional intranet or portal (Albrechtsen & Hovden, 2010). However, Katz and Lazarsfeld (1966) asserted that the distribution of cues via hardcopies may be less effective if the targeted respondents are not highly educated. According to Mangold and Faulds (2009), and Yin et al (2015), social media is the proven effective platform that could be used to enhance people's self-awareness that is related to society burning issues, irrespective of individual's demographic characteristics. Therefore, display of cues like pop-up messages and reminder notices through social media may encourage more employees to engage in practising the acceptable information security behaviours.

When a user exercise or train a particular security practice frequently, the security practice will eventually grow into a habit (Limayem, Hirt, & Cheung, 2007; Verplanken & Orbell, 2003). As information security habits construct is positively related to intention to practice information security behaviours, conducting information security training and education programs, may enhance employees' information security habits which in turn could increase their effectiveness in protecting government information systems against attacks. Other approaches that can be used to enhance information security habits include the use of cues and dialogues (Sasse et al., 2007). Dialogues pertaining

to information security issues could be used to encourage government employees' to practice information security habits. For example, in the study conducted by Albrechtsen and Hovden (2010), information security habits (such as locking computers when out of desk) had improved significantly when users were engaged in group conversations (dialogues). With regard to cues, intelligent inbuilt learning mechanisms such as regular display of a pop-up message that train and educate the employees how to identify suspicious, untrusted online resources whenever an end user visits them or to create stronger or unique passwords that are not easily hacked. In long run, the users' information security habits may improve.

Another intervention program that could be used to cultivate information security habits among Tanzania government employees is to discourage users of information systems to exercise unacceptable information security habits such as sharing of login credentials. The most widely used approach to achieve that is through security policy. The utility of security policy in shaping security habits is confirmed by Boss et al.,(2009) and Da Veiga & Eloff (2010) who found that availability of information security policy in an organisation may deter employees from performing undesired behaviours and enforce them to routinely take precautionary information security measures when using information systems. Unfortunately, the existence of information security policies in some of Tanzania government institutions is doubtful (Waziri & Yonah, 2014b). Thus, information security policies should be formulated, revised regularly and properly communicated to mandate government

employees to practice the acceptable information security habits and behaviours in general.

Another way that can be used by policy and decision makers to improve information security habits among government employees, is through curricula. Curricula can be specifically and explicitly formulated to stimulate users to attain certain information security habits or information security behaviours. This is a long-term intervention program which can be integrated into primary, secondary and higher learning institutions. Due to the fact that majority of Tanzanian higher learning institutions have no information security related courses in their curricula (Bakari et al. 2007; Nungu, 2012), the higher learning institutions should also advocate information security change or acceptance by including information security training in their academic curricula. This would ensure that future government employees are keen to exercise information security habits.

The significant impact of perceived barriers construct on the employees' intention to practice information security could lead to the growth of laxity behaviour towards the practice of information security (Claar, 2011). Thus, this finding could serve as an important indicator to policy and decision makers to strategically work on the obstacles which may prevent government employees' intention to practice information security behaviours and thwart the growth of laxity behaviour towards information security practices. Perceived barriers could be (1) technical in nature (such as checking for the origin of the web resources such as emails), which can be addressed through training; and (2)

attitudinal in nature (such as ignorance to practice information security behaviours) which can be addressed by giving more cues. Other ways to combat this problem could be issuing easy steps to perform particular information security behaviours (such as steps to identify suspicious and untrusted websites). This will help to dismiss rumours on perceived barriers in performing information security behaviours (Claar, 2011).

In addition, the imbalances between work and productivity may lead to a number of barriers to perform information security behaviours. Employees may opt to engage in unacceptable information security actions (for example, ignoring information security updates and patches) in order to expedite the achievement of certain productivity goals or to meet the deadlines (Blythe, Coventry, & Little, 2015; Rasmussen, 1997). Thus, government institutions should strike a balance between workload and productivity in order to achieve optimal information security performance.

Similar to Ajzen's (1991) proposition, the significant effect of intention in predicting employees' actual performance of information security behaviours found in this study, suggests the need for policy and decision makers to cultivate employees' intention to practice information security behaviours. Using previous studies findings, several ways can be used to increase the intention of employees to practice information security behaviours. They include provision of information security training, information security education programs, rewards, information security awareness campaigns and

information security policy (Blanke, 2008; Boss et al., 2009; D'Arcy, Hovav, & Galletta, 2009; Wiersma, 1992).

The current researcher also noted that, the effect generated by the employees' level of education qualification on intention to practice information security behaviours is mediated by the perceived severity construct. This finding suggests that employees' education level alone could not be effective in influencing the intention of the employees to practice information security behaviours, rather, its impact manifests via the perceived severity construct. Therefore, these two variables should work in tandem for the effects of employees' education level on intention to be realised. For example, if employees receive security education on the severity of information security attacks, their intention to practice information security behaviours could increase. In other words, information security education programs focusing on the severity of information security attacks could be useful for reducing the likelihood of information security attacks on government's information systems.

Nevertheless, in planning for information security training, the resident expert approach can be useful. Under this approach, in-house training could be provided to assist employees to tackle information security problems whenever the service is needed. In this way, training costs can be reduced as employees do not need to attend formal information security training courses, and the in-house training service can be continued without time limit. According to Nelson and Cheney, (1987), the resident–expert approach has proven its

advantages in terms of quality and number of people that can be trained as compared to other formal IS training approaches. A summary of major findings and policy implications are reported in table 5.1.

Table 5.1: Summary of Major Findings and Policy Implications

Major findings	Policy implication
Perceived severity and perceived susceptibility have the positive impact on information security behaviour intention.	Institutions should maintain higher levels of perceived severity and perceived susceptibility through, ICT security training, education programs, awareness campaigns and incentives/rewards.
Perceived severity could significantly mediate the impact of education level on information security behaviour intention.	Improving education and employees' security awareness on consequences of information security attacks through security education programs.
Information security habit has direct impact on employees' intention to practice security.	Improving information security habits through ICT security training, education programs, dialogues, restriction mechanisms, curricula, incentives and punishments.
Cues to action play an important role in encouraging the employees' intention to practice information security	Motivating and improving utilisation of cues through such as memos, newsletters, pop-ups, dialogues and intranet as part of tools in awareness campaigns.
The perceived barriers could discourage the employees to practice information security.	Reducing barriers to practice information security behaviour through simplicity of security technology and cues.
The intention to practice information security behaviour could motivate employees to protect government information systems	The utilisation of information security training, education programs, information security policy, rewards and security awareness campaigns could motivate employees to protect government information systems.

In general, four categories of policy implications are recommended: (1) provide more information security training, education programs and awareness campaigns; (2) disseminate more cues pertaining to good information security behaviours; (3) discourage poor information security behaviours and planning

ways to encourage the users to practice good information security behaviours and (4) formulate and update the information security policies whenever required. The recommended policy implications, when implemented, may substantially improve information security behaviours of the Tanzania government employees.

5.5 Limitations

The study has three limitations. Firstly, the use of self-reported data allows the study to examine how the studied variables could affect the perceptions of government employees on their information security behaviours. However, despite the best efforts of government employees to be as honest as possible when responding to a self-reported instrument such as the questionnaire, their responses may not be accurate due to lack of retrospective ability to produce accurate answers with regard to their behaviours (Schacter, 1999). The lack of retrospective ability is caused by limited human memory capability to accurately remember the past actions. Hence, despite its usefulness, self-reported findings should be used cautiously by decision and policy makers (Laing, Sawyer, & Noble, 1988).

Secondly, this study was conducted in Tanzania government institutions. Given the differences in respondents' personal perceptions, cultural practice differences, current ICT knowledge and level of information security awareness, it is likely that the respondents from other countries may have different perceptions on intention to practice information security behaviours

and information security behaviour itself (Alfawaz et al., 2010). Also, since the study was conducted in work setting environment which shares different characteristics (such as the existence of regulations, policies and formal ICT training) with domestic settings. Hence, the findings of this study may not be generalised in other domestic setting and other countries and hence, should be used with caution in other countries or work settings.

Thirdly, the current study is cross-sectional in nature. The results obtained from cross-sectional studies may differ over a period of time if the existing situation changes. For example, when employees are getting more education in information security, the relationship between education level and the constructs that are used to measure perceptions of benefits, barriers, susceptibility and severity may need to be re-tested. Therefore, the future studies using current research model need to be updated if the control variables such as level of awareness in information security among the studied respondents have changed.

5.6 Direction for Future Research

The limitations indicated in this study create potential research ideas which may be of interest for future research. The future studies may complement present study by investigating information security behaviours of individuals in a practical setting such as how will the studied respondents behave when responding to phishing emails, suspicious websites and malicious web links. To conduct such study, future researchers may need to use the organisation

ICT resources such as organisation networks and servers. Such kind of study can be done only if the researchers get permission and collaboration from the participating organisations. Supplementing this study with practical experiment may help to estimate discrepancies in individual's information security behaviours when measured through perceptions and in practical settings. Practical experiments may also help to overcome the limitations of the self-reported data.

The future researchers may use the current framework to study the effect of its constructs in other countries and in other domestic environment settings. Using the current research framework in future research may enrich IS literature, IS practitioners, and policy and decision makers to combat issues related to human's information security behaviours in different settings.

Additionally, future research may use the extended HBM research model to measure changes in information security behaviours in longitudinal studies. Due to the rapid changes occurring in ICT and IS field in general, conducting the similar study by measuring the extent of changes in information security behaviours over time may provide new insights in information security behaviour research.

REFERENCES

Abawajy, J. (2014). User Preference of Cyber Security Awareness Delivery Methods. *Behaviour & Information Technology*, *33*(3), 237–248.

Abraham, C. S., Sheeran, P., Abrams, D., & Spears, R. (1996). Health Beliefs and Teenage Condom Use: A Prospective Study. *Psychology and Health*, *11*(5), 641–655.

Agudelo, C. A., Bosua, R., Ahmad, A., & Maynard, S. (2016). Understanding Knowledge Leakage & BYOD (Bring Your Own Device): A Mobile Worker Perspective. In *Australasian Conference on Information Systems* (pp. 1–13). Adelaide, Australia.

Ahlan, A. R., Lubis, M., & Lubis, A. R. (2015). Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures. In *Information Systems International Conference (ISICO2015)* (Vol. 72, pp. 361–373). Surabaya, Indonesia.

Aitken, C., Roberts, P., & Jackson, G. (2010). *Fundamentals of Probability and Statistical Evidence in Criminal Proceedings: Guidance for Judges, Lawyers, Forensic Scientists and Expert Witnesses*. Royal Statistical Society's Working Group on Statistics and the Law.

Ajzen, I. (1985). *From Intentions to Actions: A Theory of Planned Behavior*. Springer.

Ajzen, I. (1991). The Theory of Planned Behavior. *Orgnizational Behavior and Human Decision Processes*, *50*(2), 179–211.

Ajzen, I., & Fishbein, M. (1980). *Understanding Attitudes and Predicting Social Behaviour*. Englewood Cliffs, New Jersey: Prentice-Hall.

Ajzen, I., & Fishbein, M. (2005). The Influence of Attitudes on Behaviour. In D. Albarracín, B. T. Johnson, & M. Zanna (Eds.), *The Handbook of Attitudes* (pp. 173–221). Mahwah, NJ: Erlbaum.

Al-Debei, M. M., Al-Lozi, E., & Papazafeiropoulou, A. (2013). Why People Keep Coming Back to Facebook: Explaining and Predicting Continuance Participation from an Extended Theory of Planned Behaviour perspective. *Decision Support Systems*, *55*(1), 43–54.

Alagbe, A. (2016). *BOYD: The Security Risks of Mobile Devices*. Strarhclyde.

Albrechtsen, E., & Hovden, J. (2010). Improving Information Security Awareness and Behaviour Through Dialogue, Participation and Collective Reflection. An Intervention Study. *Computers and Security*, *29*(4), 432–445.

Alfawaz, S., Nelson, K., & Mohannak, K. (2010). Information Security Culture : A Behaviour Compliance Conceptual Framework. In *8th Australasian Information Security Conference* (Vol. 105, pp. 47–55). Brisbane, Australia.

Ali, M., Haidar, N., Ali, M. M., & Maryam, A. (2011). Determinants of Seat Belt use Among Drivers in Sabzevar, Iran: A comparison of Theory of Planned Behavior and Health Belief Model. *Traffic Injury Prevention*, *12*(1), 104–109.

Amir, W. (2016). The Online Hacktivist Anonymous has Breached into the Server of aTanzanian Telecom Firm and Leaked Personal Data of about 64,000 Employees. Retrieved July 10, 2016, from https://www.hackread.com/anonymous-opafrica-tanzanian-telecom-firm-hacked/

Anderson, J. C., Gerbing, D. W., & Hunter, J. E. (1987). On the Assessment of Unidimensional Measurement: Internal and External Consistency, and Overall Consistency Criteria. *Journal of Marketing Research*, *24*(4), 432–437.

Ando, R., Shima, S., & Takemura, T. (2016). Analysis of Privacy and Security Affecting the Intention of Use in Personal Data Collection in an IoT Environment. *IEICE Transactions on Information and Systems*, *E99D*(8), 1974–1981.

Andrews, D., Nonnecke, B., & Preece, J. (2003). Electronic Survey Methodology: A Case Study in Reaching Hard-to-Involve Internet Users. *International Journal of Human-Computer Interaction*, *16*(2), 185–210.

Ani, U. P. D., He, H. M., & Tiwari, A. (2017). Human Capability Evaluation Approach for Cyber Security in Critical Industrial Infrastructure. In *Advances in Human Factors in Cybersecurity* (pp. 169–182). Los Angels, USA: Springer.

Armitage, C., & Conner, M. (2001). Efficacy of the Theory of Planned Behaviour: A Meta-Analytic Review. *The British Journal of Social Psychology*, *40*(4), 471–499.

Armitage, C. J., & Conner, M. (2000). Social Cognition Models and Health Behaviour: A structured Review. *Psychology and Health*, *15*(2), 173–189.

Awang, Z. (2015). *SEM Made Simple: A Gentle Approach to Learning Structural Equation Modeling*. Selangor, Kuala Lumpur: MPWS Rich Publication.

Bada, M., & Sasse, A. (2014). Cyber Security Awareness Campaigns: Why do they fail to change Behaviour? Global Cyber Security Capacity Centre, University of Oxford.

Bagozzi, R. (1981). Unobservable Variables and Measurement. *Journal of Marketing Research*, *18*, 375–382.

Bakari, J. K. (2013). Delivering Secure, Public-Oriented e-GovernmentFacilities in Africa: A Holistic Approach. In *The 7th annual e-Gov Forum of the Commonwealth Telecommunications Organisation*. Kampala, Uganda: CTO.

Bakari, J. K., Magnusson, C., Yngström, L., & Tarimo, C. N. (2007). Operationalization of ICT security Policy, Services and Mechanisms in Organizations. In *Proceedings of IST Africa*. Maputo, Mozambique: IST.

Bakari, J. K., Tarimo, C. N., Yngstrom, L., & Magnusson, C. (2005). State of ICT security Management in the Institutions of Higher Learning in Developing Countries: Tanzania Case Study. In *Fifth IEEE International Conference on Advanced Learning Technologies(ICALT 2005)* (pp. 1007–1011). Kaohsiung, Taiwan.

Baker, T. (1994). *Doing Social Research* (2nd Ed). New York, USA: McGraw-Hill Inc.

Bandura, A. (1977). Self-efficacy: Toward a Unifying Theory of Behavioral Change. *Psychological Review*, *84*(2), 191.

Banerjee, C., & Pandey, S. K. (2010). Research on Software Security Awareness. *ACM SIGSOFT Software Engineering Notes*, *35*(5), 1.

Baptista, G., & Oliveira, T. (2017). Why so serious? Gamification impact in the acceptance of mobile banking services. *Internet Research*, *27*(1), 118–139.

Baptista, G., Oliveira, T., Hong, W., Thong, J. Y. L., Chasalow, L. C., & Dhillon, G. (2011). User Acceptance of Agile Information Systems: A Model and Empirical Test. *Journal of Management Information Systems*, *28*(1), 235–272.

Bargh, J. A. (1994). *The Four Horsemen of Automaticity: Intention, Awareness, Efficiency, and Control as Separate Issues*. (R. Wyer & T. Srull, Eds.)*Handbook of Social Cognition.* Lawrence Erlbaum Associates.

Baron, R., & Kenny, D. (1986). The Moderator–Mediator Variable Distinction in Social Psychological Research: Conceptual, Strategic, and Statistical Considerations. *Journal of Personality and Social Psychology*, *51*(6), 1173.

Barrett, L., Henzi, S. P., Weingrill, T., Lycett, J. E., & Hill, R. A. (1999). Market Forces Predict Grooming Reciprocity in Female Baboons. *Proceedings of the Royal Society B: Biological Sciences*, *266*(1420), 665–670.

Barrett, P. (2007). Structural Equation Modelling: Adjudging Model Fit. *Personality and Individual Differences*, *42*(5), 815–824.

Becker, M., Maiman, L. A., Kirscht, J. P., Haefner, D. P., & Drachman, R. (1977). The Health Belief Model and prediction of dietary compliance: a field experiment. *Journal of Health and Social Behavior*, *18*(4), 348–366.

Bentler, P. M., & Bonett, D. G. (1980). Significance Tests and Goodness of Fit in the Analysis of Covariance Structures. *Psychological Bulletin*, *88*(3), 588.

Bentler, P. M., & Chou, C.-P. (1987). Practical Issues in Structural Modeling. *Sociological Methods & Research*, *16*(1), 78–117.

Bentler, P. M., & Wu, E. J. C. (2005). *EQS 6.1 for Windows*. *Structural Equations Program Manual*. Encino, CA: Multivariate Software Inc.

Bentler, P., & Yuan, K.-H. (1999). Structural Equation Modeling with Small Samples: Test Statistics. *Multivariate Behavioral Research*, *34*(2), 181–197.

Biggs, J., Kember, D., & Leung, D. Y. P. (2001). The Revised Two-Factor Study Process Questionnaire: R-SPQ-2F. *British Journal of Educational Psychology*, *71*(1), 133–149.

Birba, O., & Diagne, A. (2012). Determinants of Adoption of Internet in Africa: Case of 17 sub-Saharan countries. *Structural Change and Economic Dynamics*, *23*(4), 463–472.

Blanke, S. J. (2008). A Study of the Contributions of Attitude, Computer Security Policy Awareness, and Computer Self-Efficacy to the Employees' Computer Abuse Intention in Business Environments. Nova Southeastern University.

Blanthorne, C., Jones-Farmer, A., & Almer, E. (2006). Why you Should Consider SEM: A Guide to Getting Started. In V. Arnold (Ed.), *Advances in Account Behavioural Studies* (pp. 179–207). Amsterdam: Elsevier B.V.

Bleiker, E. M., Menko, F. H., Taal, B. G., Kluijt, I., Wever, L. D. V, Gerritsma, M., … Aaronson, N. K. (2005). Screening Behavior of Individuals at High Risk for Colorectal Cancer. *Gastroenterology*, *128*(2), 280–287.

Blythe, J., Coventry, L., & Little, L. (2015). Unpacking security policy compliance: The motivators and barriers of employees' security behaviors. In *Symposium On Usable Privacy and Security (SOUPS). USENIX Association, Ottawa* (pp. 103–122).

Böhme, R., & Moore, T. (2016). The "Iterated Weakest Link" Model of Adaptive Security Investment. *Journal of Information Security*, *7*, 81–102.

Bollen, K. A. (1989a). A new Incremental Fit Index for General Structural Equation Models. *Sociological Methods & Research*, *17*(3), 303–316.

Bollen, K. A. (1989b). *Strucrural Equations with Latent Variables.* New York: Willey.

Bollen, K. A., & Stine, R. (1990). Direct and indirect effects: Classical and bootstrap estimates of variability. *Sociological Methodology*, *20*(1), 15–140.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. a, & Boss, R. W. (2009). If someone is Watching, I'll do what I'm asked: Mandatoriness, Control, and Information Security. *European Journal of Information Systems*, *18*(2), 151–164.

Bourg, K. A. (2014). *An Exploration of the Factors Influencing Home User's Cybersecurity Factors*. *PhD Thesis*. Victoria University of Wellington.

Bowen, P., Chew, E., & Hash, J. (2007). Information Security Guide For Government Executives. Gaithersburg: NIST.

Bradley, L., & Prentice, G. (2017). Consumer to Consumer (C2C) Online Auction Transaction Intentions : an Application of the Theory of Planned Behaviour. *DBS Business Review*, *1*, 5–25.

Braun, V., & Clarke, V. (2006). Using Thematic Analysis in Pyschology. *Qualitative Research in Psychology*, *3*(2), 77–101.

Brewer, N. T., Chapman, G. B., Gibbons, F. X., Gerrard, M., McCaul, K. D., & Weinstein, N. D. (2007). Meta-Analysis of the Relationship Between Risk Perception and Health Behavior: The Example of Vaccination. *Health Psychology*, *26*(2), 136–145.

Broom, A., & Willis, E. (2007). Competing Paradigms and Health Research. In *Researching health: Qualitative, Quantitative and Mixed methods* (pp. 16–30). London,UK: Sage London.

Brown, L. K., DiClemente, R. J., & Park, T. (1992). Predictors of Condom Use in Sexually Active Adolescents. *Journal of Adolescent Health*, *13*(8), 651–657.

Buckley, M. R., Cote, J. A., & Comstock, S. M. (1990). Measurement Errors in the Behavioral Sciences: The case of Personality/Attitude Research. *Educational and Psychological Measurement*, *50*(3), 447–474.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, *34*(3), 523–548.

Byrne, B. M. (2009). *Structural Equation Modeling with AMOS: Basic Concepts, Applications, and Programming* (Second Ed). New York: Routledge.

Campbell, J. P. (1982). Editorial: Some Remarks from the Outgoing Editor. *Journal of Applied Psychology*, *67*, 691–700.

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of Information Security at the Workplace : Linking Information Security Climate to Compliant Behavior. *Journal of Information Privacy and Security*, *1*(3), 18–41.

Chang, S.-J., Van Witteloostuijn, A., & Eden, L. (2010). From the editors: Common Method Variance in International Business Research. *Journal of International Business Studies*, *41*(2), 178–184.

Chen, C. (2003). *An Investigation of Significant Factors Affecting Consumer Trust in E-commerce*. University of Nevada, Las Vegas.

Cheney, M. K., & John, R. (2013). Underutilization of Influenza Vaccine : A Test of the Health Belief Model. *Sage Open*, *3*(2).

Chenoweth, T., Minch, R., & Gattiker, T. (2009). Application of protection motivation theory to adoption of protective technologies. In *System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference on* (pp. 1–10). Hawaii.

Cheung, G. W., & Lau, R. S. (2007). Testing Mediation and Suppression Effects of Latent Variables: Bootstrapping with Structural Equation Models. *Organizational Research Methods*, *11*(296–325).

Chuang, B. K., Tsai, C. H., Hsieh, H. L., & Tumurtulga, T. (2013). Applying Health Belief Model to Explore the Adoption of Telecare. In *12th International Conference on Computer and Information Science(ICIS 2013)* (pp. 269–272). Toki Messe, Japan: IEE.

Citzen. (2014). Delayed refunds anger victims of ATM theft. Dar es Salaam, Tanzania. Retrieved from http://www.thecitizen.co.tz/News/Delayed-refunds-anger-victims-of-ATM-theft/-/1840392/2483584/-/x9m1ixz/-/index.html

Claar, C. (2011). *The Adoption of Computer Security: An Analysis of Home Personal Computer User Behavior Using the Health Belief Model*. Utah State University, USA.

Claar, C., & Johnson, J. (2012). Analyzing Home PC Security Adoption Behavior. *Journal of Computer Information Systems*, *52*(4), 20–29.

Cochran, W. (1977). *Sampling Techniques* (3rd Ed). New York: John Wiley & Sons.

Cohen, J. (1988). *Statistical Power Analysis for the Behavioral Sciences* (2nd ed.). NJ: Erlbaum: Hillsdale.

Conner, M., & Armitage, C. J. (1998). Extending the Theory of Planned Behavior: A Review and Avenues for Further Research. *Journal of Applied Social Psychology, 28*, 1429–1464.

Cook, R. D. (1977). Detection of influential observation in linear regression. *Technometrics*, *19*(1), 15–18.

Costello, A., & Osborne, J. (2005). Best Practices in Exploratory Factor Analysis: Four Recommendations for Getting the Most from your Analysis. *Practical Assessment Reseach & Evaluation.*, *10*(7), 1–8.

Couper, M. (2000). Web Surveys: A Review of Issues and Approaches. *Web Surveys: A Review of Issues and Approaches*, *64*(4), 464–494.

Craighead, C., Ketchen, D., Dunn, K., & Hult, T. (2011). Addressing common method variance: guidelines for survey research on information technology, operations, and supply chain management. *IEEE Transactions on Engineering Management*, *58*(3), 578–588.

Creswell, J. W. (2012). *Qualitative Inquiry and Research Design: Choosing among five Approaches* (3rd Ed). London: Sage.

Creswell, J. W. (2013). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (4th Ed). London: Sage publications.

Creswell, J. W., & Clark, V. L. P. (2007). *Designing and Conducting Mixed Methods Research*. Thousand Oaks: Sage Publications, Inc.

Crossler, R., & Belanger, F. (2014). An Extended Perspective on Individual Security Behaviors : Protection Motivation Theory and a Unified Security Practices (USP) Instrument. *The Database for Advances in Information Systems*, *45*(4), 51–71.

Crossler, R. E. (2010). Protection Motivation Theory: Understanding Determinants to Backing up Personal Data. In *System Sciences (HICSS), 2010 43rd Hawaii International Conference on System Sciences* (pp. 1–10).

Crossler, R., Long, A., Loraas, T., & Trinkle, B. (2014). Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems*, *28*(1), 209–226.

Crotty, M. (1998). *The Foundations of Social Research: Meaning and Perspective in the Research Process*. Sage.

Cudeck, R., & O'Dell, L. L. (1994). Applications of standard error estimates in unrestricted factor analysis: significance tests for factor loadings and correlations. *Psychological Bulletin*, *115*(3), 475.

Curran, P. J., West, S. G., & Finch, J. F. (1996). The Robustness of Test Statistics to Nonnormality and Specification Error in Confirmatory Factor Analysis. *Psychological Methods*, *1*(1), 16.

Czaja, S. J., Guerrier, J. H., Nair, S. N., & Landauer, T. K. (1993). Computer Communication as an aid to Independence for Older Adults. *Behaviour & Information Technology*, *12*(4), 197–207.

Czaja, S., & Sharit, J. (1998). Age Differences in Attitudes Toward Computers. *The Journals of Gerontology. Series B, Psychological Sciences and Social Sciences*, *53*(5), 329–340.

D'Arcy, John & Hovav, A. (2004). The Role of Individual Characteristics on the Effectiveness of IS Security Countermeasures on the Effectiveness of IS Security Countermeasures. In *Proceedings of the Tenth Americas Conference on Information Systems (AMCIS 2004)* (pp. 1395–1402). 6-8 August 2004 New York, USA: AISEL.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79–98.

Da Veiga, A., & Eloff, J. H. P. (2010). A Framework and Assessment Instrument for Information Security Culture. *Computers and Security*, *29*(2), 196–207.

Daniel, W. W. (1999). *Biostatistics: A Foundation for Analysis in the Health Sciences*. *New York* (7th Ed). New York: John Wiley & Sons.

Davern, M. (2011). Representative Sample. In P. J. Lavrakas (Ed.), *Encyclopedia of Survey Research Methods*. Sage Publications, Inc.

Davinson, N., & Sillence, E. (2010). It Won't Happen to me: Promoting Secure Behaviour Among Internet Users. *Computers in Human Behavior*, *26*(6), 1739–1747.

Davinson, N., & Sillence, E. (2014). Using the Health Belief Model to Explore Users' Perceptions of "Being Safe and Secure" in the World of Technology Mediated Financial Transactions. *International Journal of Human Computer Studies*, *72*(2), 154–168.

Denzin, N. K., & Lincoln, Y. S. (2011). *The Sage Handbook of Qualitative Research*. London: Sage.

Dewa, M., & Zlotnikova, I. (2014). Current Status of e-Government Services in Tanzania : A Security Perspective. *ACSIJ Advances in Computer Science : An International Journal*, *3*(3), 114–122.

Diamantopoulos, A., Siguaw, J. A., & Siguaw, J. A. (2000). *Introducing LISREL: A guide for the uninitiated*. Sage.

Diatmika, I. W. B., Irianto, G., & Baridwan, Z. (2016). Determinants of Behavior Intention Of Accounting Information Systems Based Information Technology Acceptance. *Imperial Journal of Interdisciplinary Research*, *2*(8), 125–138.

DiIorio, C. K. (2005). *Measurement in Health Behavior: Methods for Research and Evaluation*. San Fransisco, USA: Jossey Bass.

Dikko, M. (2016). Establishing Construct Validity and Reliability: Pilot Testing of a Qualitative Interview for Research in Takaful (Islamic Insurance). *The Qualitative Report*, *21*(3), 521.

DiMatteo, M. R., Haskard, K. B., & Williams, S. L. (2007). Health Beliefs, Disease Severity, and Patient Adherence. *Medical Care*, *45*(6), 521–528.

Dincelli, E. (2017). Can Privacy and Security Be Friends ? A Cultural Framework to Differentiate Security and Privacy Behaviors on Online Social Networks. *Proceedings of the 50th Hawaii International Conference on System Sciences*, 4011–4020.

Dinev, T. (2008). Internet Users' Beliefs about Government Surveillance The Role of Social Awareness and Internet Literacy. In *Proceedings of the 41st Annual Hawaii International Conference on System Sciences* (p. 275). 7-10 January 2008 Honolulu, Hawaii.

Dinev, T., & Hu, Q. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. *Journal of the Association for Information Systems*, *8*(7), 386–408.

Do, C. B., & Batzoglou, S. (2008). What is the Expectation Maximization Algorithm? *Nature Biotechnology*, *26*(8), 897–899.

Domasa, S. (2017). Better Services Beckon as Digitized Systems kick off. *Daily News*, pp. 1–3. Dodoma.

Dowland, P., Furnell, S., Illingworth, H., & Reynolds, P. (1999). Computer Crime and Abuse: A Survey of Public Attitudes and Awareness. *Computers and Security*, *18*(8), 715–728.

Easterby-Smith, M., Thorpe, R., & Jackson, P. (2012). *Management research* (4th Ed). London: Sage.

Eccles, M. P., Hrisos, S., Francis, J., Kaner, E. F., Dickinson, H. O., Beyer, F., & Johnston, M. (2006). Do self-reported intentions predict clinicians' behaviour: a systematic review. *Implementation Science*, *1*(1), 28.

Ede, A., Hwang, S., & Feltz, D. L. (2011). Current Directions in Self-efficacy Research in Sport. *Revista Iberoamericana de Psicología Del Ejercicio Y El Deporte*, *6*(2), 181–202.

Edwards, J. (1992). A Cybernetic Theory of Stress and Coping. *Academy of Management Review*, *17*(2), 238–274.

Edwards, R., & Engelhardt, K. (1989). Microprocessor-Based Innovations and Older Individuals: AARP Survey Results and their Implications for Service Robotics. *International Journal of Technology & Aging*, *2*(1), 42–55.

El Aziz, R. A., El Badrawy, R., & Hussien, M. I. (2014). ATM, Internet Banking and Mobile Banking Services in a Digital Environment: The Egyptian Banking Industry. *International Journal of Computer Applications*, *90*(8), 45–52.

Escobar-Rodríguez, T., Carvajal-Trujillo, E., & Monge-Lozano, P. (2014). Factors that influence the perceived advantages and relevance of Facebook as a learning tool: An extension of the UTAUT. *Australasian Journal of Educational Technology*, *30*(2), 136–151.

Fabrigar, L. R., Wegener, D. T., MacCallum, R. C., & Strahan, E. J. (1999). Evaluating the Use of Exploratory Factor Analysis in Psychological Research. *Psychological Methods*, *4*(3), 272–299.

Falk, F., & Miller, N. (1992). *A Primer for Soft Modeling.* Akron, OH, US: University of Akron Press.

Fincham, J. E. (2008). Response Rates and Responsiveness for Surveys, Standards, and the Journal. *American Journal of Pharmaceutical Education*, *72*(2), 43.

Fishman, J. A., & Galguera, T. (2003). *Introduction to Test Construction in the Social and Behavioral Sciences: A Practical Guide* (Ist Ed). Maryland, UK: Rowman & Littlefield Publishers.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A Meta-Analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology*, *30*(2), 407–429.

Fornell, C., & Larcker, D. F. (1981). Structural Equation Models with Unobservable Variables and Measurement Rrror: Algebra and Statistics. *Journal of Marketing Research*, *18*(3), 382–388.

Friborg, O., Hjemdal, O., Rosenvinge, J. H., & Martinussen, M. (2003). A New Rating Scale for Adult Resilience: What are the Central Protective Resources Behind Healthy Adjustment? *International Journal of Methods in Psychiatric Research*, *12*(2), 65–76.

Fritz, M. S., & MacKinnon, D. P. (2007). Required Sample Size to Detect the Mediated Effect. *Psychological Science*, *18*(3), 233–239.

Furnell, S., & Clarke, N. (2005). Organizational Security Culture: Embedding Security Awareness, Education, and Training. In *Proceedings of the 4th World Conference on Information Security Education* (Vol. 11, pp. 67–74). Moscow.

Gahnström, C. S. (2012). *Ethnicity, religion and politics in Tanzania: The 2010 general elections and Mwanza region*.

Ganster, D. C., Hennessey, H. W., & Luthans, F. (1983). Social Desirability Response Effects: Three Alternative Models. *Academy of Management Journal*, *26*(2), 321–331.

Gao, X., Nau, D. P., Rosenbluth, S. A., Scott, V., & Woodward, C. (2000). The Relationship of Disease Severity, Health Beliefs and Medication Adherence among HIV Patients. *AIDS Care*, *12*(4), 387–398.

Gaskin, J. (2012). Confirmatory Factory Analysis: Common Latent Factor. Retrieved July 17, 2016, from http://statwiki.kolobkreations.com/index.php?title=Confirmatory_Factor_Analysis#Common_Latent_Factor

Gentile, A. (1975). *Physcian Visits: Volume and Interval Since Last Visit*. Washington, DC, USA.

Gibbs, J. P. (1968). Crime, Punishment, and Deterrence. *The Southwestern Social Science Quarterly*, *48*(4), 515–530.

Gibbs, L. (2007). *An Analyis of Adults African American Men's Perceived Susceptibility of Prostate cancer and Perceived Benefits and Barriers to Participation in Early Detection Methods: Implications for Community - Based Health Promotions*. Nothern Illinois University.

Gicheru, E. (2013). The Psychology of Unmarried Men in Nairobi: A case Study of three Bachelors over forty. *African Journal of History and Culture*, *5*(6), 126.

Glanz, K., Rimer, B. K., & Viswanath, K. (2008). *Health Behavior and Health Education: Theory, Research, and Practice* (4th Ed). San Fransisco, USA: John Wiley & Sons.

Goldfarb, A., & Prince, J. (2008). Internet Adoption and Usage Patterns are Different: Implications for the Digital Divide. *Information Economics and Policy*, *20*(1), 2–15.

Gonalves, C., Biscaia, R., Correia, A., & Diniz, A. (2014). An Examination of Intentions of Recommending Fitness Centers by User Members. *Motriz. Revista de Educacao Fisica*, *20*(4), 384–391.

Graham, J. W., Hofer, S. M., & MacKinnon, D. P. (1996). Maximizing the Usefulness of Data obtained with Planned Missing Value Patterns: An Application of Maximum Likelihood Procedures. *Multivariate Behavioral Research*, *31*(2), 197–218.

Grant, G. J. (2010). *Ascertaining the Relationship Between Security Awareness and the Security Behavior of Individuals*. Nova Southeastern University.

Gratton, C., & Jones, I. (2010). *Research Methods for Sports Studies*. Taylor & Francis.

Guba, E. G., & Lincoln, Y. S. (1994). Competing Paradigms in Qualitative Research. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of qualitative research* (Vol. 2, p. 105). Thousand Oaks: Sage, Thousand Oaks, CA.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a Silver Bullet. *The Journal of Marketing Theory and Practice*, *19*(2), 139–152.

Hair Jr, J., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate Data Analysis* (7th Ed). London,UK: Prentice-Hall.

Hanus, B., & Wu, Y. "Andy." (2016). Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management*, *33*(1), 2–16.

Hassan, R. G., & Khalifa, O. O. (2016). E-Government - an Information Security Perspective. *International Journal of Computer Trends and Technology*, *36*(1), 1–9.

Hayduk, L. (1987). *Structural Equation Modelling with LISREL*. Baltmore: John Hopkins University Press.

Hayes, A. F. (2013). *Introduction to Mediation, Moderation, and Conditional Process Analysis: A Regression-Based Approach*. Guilford Press.

Hayes, A. F. (2016). *Partial, Conditional, and Moderated Moderated Mediation: Quantification, Inference, and Interpretation*. *Manuscript submitted for publication*.

Heirman, W., & Walrave, M. (2012). Predicting Adolescent Perpetration in Cyberbullying: An Application of the Theory of Planned Behavior. *Psicothema*, *24*(4), 614–620.

Henderson, S. (2005). The Neglect of Volition. *British Journal of Psychiatry*, *186*, 273–274.

Henning, E., Van Rensburg, W., & Smit, B. (2004). *Finding your Way in Qualitative Research*. Pretoria: Van Schaik.

Herath, C. S. (2013). Does Intention Lead to Behaviour? A Case Study of the Czech Republic Farmers. *Agricultural Economics*, *59*(3), 143–148.

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. (2014). Security Services as Coping Mechanisms: An Investigation into User Intention to Adopt an Email Authentication Service. *Information Systems Journal*, *24*(1), 61–84.

Herath, T., & Rao, H. R. (2009). Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations. *European Journal of Information Systems*, *18*, 106–125.

Hingson, R. W., Strunin, L., Berlin, B. M., & Heeren, T. (1990). Beliefs About AIDS, Use of Alcohol and Drugs, and Unprotected Sex Among Massachusetts Adolescents. *American Journal of Public Health*, *80*(3), 295–299.

Hochbaum, G. M. (1958). *Public Participation in Medical Screening Programs: A Socio-Psychological Study*. Washington, USA: US Department of Health, Education, and Welfare, Public Health Service, Bureau of State Services, Division of Special Health Services, Tuberculosis Program,.

Holbrook, A., Krosnick, J. A., & Pfent, A. (2007). The Causes and Consequences of Response Rates in Surveys by the News Media and Government Contractor Survey Research Firms. In J. Lepkowski, C. Tucker, M. Brick, E. de Leeuw, L. Japec, P. J. Lavrakas, … R. L. Sangster (Eds.), *Advances in Telephone Survey Methodology* (pp. 499–528). Wiley Hoboken, NJ.

Horst, M., Kuttschreuter, M., & Gutteling, J. M. (2007). Perceived Usefulness, Personal Experiences, Risk Perception and Trust as Determinants of Adoption of e-Government Services in The Netherlands. *Computers in Human Behavior*, *23*(4), 1838–1852.

Hsu, C., & Huang, S. (2010). Formation of Tourist Behavioral Intention and Actual Behavior. In *7th International Conference on Service Systems and Service Management (ICSSSM)* (pp. 1–6).

Hu, L., & Bentler, P. M. (1998). Fit indices in covariance structure modeling: Sensitivity to underparameterized model misspecification. *Psychological Methods*, *3*(4), 424.

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM*, *54*(6), 54–60.

Hudson, J. M., & Bruckman, A. (2004). "Go away": Participant Objections to Being Studied and the Ethics of Chatroom Research. *The Information Society*, *20*(2), 127–139.

Hufnagel, E. M., & Conca, C. (1994). User Response Data: The potential for Errors and Biases. *Information Systems Research*, *5*(1), 48–73.

Humaidi, N., & Balakrishnan, V. (2012). The Influence of Security Awareness and Security Technology on Users ' Behavior towards the Implementation of Health Information System : A Conceptual Framework. In *2nd International Conference on Management and Artificial Intelligence* (Vol. 35, pp. 1–6). Bangkok, Thailand: IACSIT Press.

Ifinedo, P. (2012). Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory. *Computers and Security*, *31*(1), 83–95.

Innami, Y., & Koizumi, R. (2013). *Structural Equation Modeling in Education Research : A Primer*. (M. Khine, Ed.)*Application of Structural Equation Modeling in Educational Research and Practice*. Sense Publishers.

Jansen, J., & Schaik, P. (2016). Understanding Precautionary Online Behavioural Intentions : A Comparison of Three Models. In *Human Aspects of Information Security & Assurance (HAISA 2016)* (pp. 1–11). Frankfurt, Germany.

Jansen, J., & van Schaik, P. (2016). Understanding Precautionary Online Behavioural Intentions: A Comparison of Three Models. In *HAISA* (pp. 1–11). Frankfurt, Germany.

Janz, N. K., & Becker, M. H. (1984). The Health Belief Model: A Decade Later. *Health Education Quarterly*, *11*(1), 1–47.

Jenkins, J., Durcikova, A., & Burns, M. (2011). Get a cue on is Security Training: Explaining the Difference between how Security Cues and Security Arguments Improve Secure Behavior. In *Thirty Second International Conference on Information Systems* (pp. 1–11). Shanghai.

Jia, L., & Hall, D. (2014). The Effect of Technology Usage Habits on Consumers ' Intention to Continue Use Mobile Payments. In *Twentieth Americas Conference on Information Systems* (pp. 1–12). Savannah, USA.

Johnson, D. R., & Creech, J. (1984). Ordinal Measures in Multiple Indicator Models : A Simulation Study of Categorization Error. *American Sociological Review*, *48*(3), 398–407.

Johnston, A. C., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly*, *34*(3), 549–566.

Johnston, B. A. C., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviours : An Impirical Study. *MIS Quarterly*, *34*(3), 549–566.

Kaiser, H. F. (1970). A Second generation Little Jiffy. *Psychometrika*, *35*(4), 401–415.

Karokola, G. (2010). *A Systemic Analysis of e-Government Maturity Models: The Need for Security Services - A Case of Developing Regions*. University of Stockholm/Royal Institute of Technology.

Karokola, G., Kowalski, S., & Yngström, L. (2011). Towards An Information Security Maturity Model for Secure e-Government Services : A Stakeholders View. *Proceedings of the 5th HAISA 2011 Conference, London, UK*, 58--73.

Kegeles, S. S., Kirscht, J. P., Haefner, D. P., & Rosenstock, I. M. (1965). Survey of Beliefs about Cancer Detection and Taking Papanicolaou Tests. *Public Health Reports*, *80*(9), 815–823.

Kemery, E. R., & Dunlap, W. P. (1986). Partialling factor scores does not control method variance: A reply to Podsakoff and Todor. *Journal of Management*, *12*(4), 525–530.

Khan, B., Alghathbar, K., & Khan, M. (2011). Information Security Awareness Campaign : An Alternate Approach. In *Communications in Computer and Information Science* (pp. 1–10). Brno, Czech Republic.

Kim, W. (2010). *Managerial Coaching Behavior and Employee Outcomes: A Structural Equation Modeling Analysis*. Texas A&M University.

Kline, B. (2005). *Principles and Practice of Structural Equation Modeling* (2nd ed.). New York, USA: The Guilford Press.

Krueger, C., & Tian, L. (2004). A Comparison of the General Linear Mixed Model and Repeated Measures ANOVA Using a Dataset with Multiple Missing Data Points. *Biological Research for Nursing*, *6*(352), 151–157.

Laing, J., Sawyer, R., & Noble, J. (1988). *Accuracy of self-reported activities and accomplishments of college-bound students*. Iowa City, IA: American College Testing Program.

Lankton, N. K., McKnight, D. H., & Thatcher, J. B. (2012). The Moderating Effects of Privacy Restrictiveness and Experience on Trusting Beliefs and Habit: An Empirical Test of Intention to Continue using a Social Networking Website. *IEEE Transactions on Engineering Management*, *59*(4), 654–665.

LaRose, R., & Rifon, N. J. (2007). Promoting e-Safety: Effects of Privacy warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior. *Journal of Consumer Affairs*, *41*(1), 127–149.

Lazarus, R. (1993). Coping Theory and Research: Past, Present and Future. *Psychosomatic Medicine*, *247*(55), 234–247.

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our Network Safe: A Model of Online Protection Behaviour. *Behaviour & Information Technology*, *27*(5), 445–454.

Lee, M. (2013). *Exercise Barriers in Cancer Survivors: A Multi-Dimensional Approach*. University of South Florida, USA.

Lee, Y., & Larsen, K. (2009). Threat or Coping Appraisal: Determinants of (SMB) Executives Decision to Adopt Anti-malware Software. *European Journal of Information Systems*, *18*(2), 177–187.

Leedy, P. N., & Ormrod, J. E. (2005). *Practical research: Planning and Design* (8th ed.). Upper Saddle River, NJ: Pearson Prentice Hall.

Lévesque, F. L., Fernandez, J., & Batchelder, D. (2017). Age and gender as independent risk factors for malware victimisation. In *Proceedings of the 31th International British Human Computer Interaction Conference (BHCI)* (pp. 1–14).

Li, H., Zhang, J., & Sarathy, R. (2010). Understanding Compliance with Internet Use Policy from the Perspective of Rational Choice Theory. *Decision Support Systems*, *48*(4), 635–645.

Li, Y. (2015). *Users' Information Systems (IS) Security Behavior in Different Contexts*. Oulu, Finland.

Lian, J.-W., & Yen, D. C. (2014). Online shopping drivers and barriers for older adults: Age and gender differences. *Computers in Human Behavior*, *37*, 133–143.

Liang, H., & Xue, Y. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly*, *33*(1), 71–90.

Liang, H., & Xue, Y. (2010). Understanding Security Behaviors in Personal Computer Usage : A Threat Avoidance Perspective. *Journal of the Association for Information Systems*, *11*(7), 394–413.

Liao, C., Palvia, P., & Lin, H.-N. (2006). The Roles of Habit and Website Quality in e-Ecommerce. *International Journal of Information Management*, *26*(6), 469–483.

Lieberman, P. E. (2010). Deterrence Theory. *Billboard*, *1*(1971), 8–8.

Limayem, M., Hirt, S. G., & Cheung, C. M. K. (2007). How Habit Limits the Predictive Power of Intention: The Case of Information Systems Continuance. *Mis Quarterly*, *31*(4), 705–737.

Limayem, M., Khalifa, M., & Chin, W. W. (2004). Factors Motivating Software Piracy: A Longitudinal Study. *IEEE Transactions on Engineering Management*, *51*(4), 414–425.

Little, R. J. A. (1988). A Test of Missing Completely at Random for Multivariate Data with Missing Values. *Journal of the American Statistical Association*, *83*(404), 1198–1202.

Liu, K. (1988). Measurement Error and its Impact on Partial Correlation and Multiple Linear Regression Analyses. *American Journal of Epidemiology*, *127*(4), 864–874.

Longo, D. A., Lent, R. W., & Brown, S. D. (1992). Social Cognitive Variables in the Prediction of Client Motivation and Attrition. *Journal of Counseling Psychology*, *39*(4), 447–452.

Lupilya, E. C., & Jung, K. (2015). E-Government Transformation in Tanzania : Status , Opportunities , and Challenges. *The Korean Journal of Policy Studies*, *30*(1), 147–184.

Lüthje, C., & Franke, N. (2003). The "Making"of an Entrepreneur: Testing a Model of Entrepreneurial Intent Among Engineering Students at MIT. *R&D Management*, *33*(2), 135–147.

Lwanga, S. K., & Lemeshow, S. (1991). *Sample Size Determination in Health Studies: A Practical Manual*. Geneva: World Health Organization.

Mackenzie, N., & Knipe, S. (2006). Research Dilemmas: Paradigms, Methods and Methodology. *Issues in Educational Research*, *16*(2), 193–205.

MacKinnon, D. P., Lockwood, C. M., Hoffman, J. M., West, S. G., & Sheets, V. (2002). A comparison of methods to test mediation and other intervening variable effects. *Psychological Methods*, *7*(1), 83.

Maguire, K., & Lizewski, L. (2010). The Health Belief Model. Retrieved August 7, 2015, from http://lawrencelizewski.com/attachments/File/HBM.pdf

Mahabi, V. (2010). *Florida State University Libraries Information Security Awareness : System Administrators and End-User Perspectives at Florida State University*. Florida State University.

Malhotra, N. K., Kim, S. S., & Patil, A. (2006). Common method variance in IS research: A comparison of alternative approaches and a reanalysis of past research. *Management Science*, *52*(12), 1865–1883.

Mangold, W. G., & Faulds, D. J. (2009). Social Media: The new Hybrid Element of the Promotion Mix. *Business Horizons*, *52*(4), 357–365.

Marczyk, G., DeMatteo, D., & Festinger, D. (2005). *Essentials of Research Design and Methodology*. New Jersey: John Wiley & Sons Inc.

Marquaridt, D. W. (1970). Generalized inverses, Ridge Regression, Biased Linear Estimation, and Non-linear Estimation. *Technometrics*, *12*(3), 591–612.

Marsh, H. W., Hau, K.-T., & Wen, Z. (2004). In search of golden rules: Comment on hypothesis-testing approaches to setting cutoff values for fit indexes and dangers in overgeneralizing Hu and Bentler's (1999) findings. *Structural Equation Modeling*, *11*(3), 320–341.

Masa'deh, R. (Moh'd T., Tarhini, A., Mohammed, B. A., & Maqableh, M. (2016). Modeling Factors Affecting Student's Usage Behaviour of E-Learning Systems in Lebanon. *International Journal of Business and Management*, *11*(2), 299.

Maumbe, B., & Owei, V. (2012). Understanding the Information Security Landscape in South Africa: Implications for Strategic Collaboration. In B. Maumbe (Ed.), *E-Agriculture and Rural Development: Global Innovations and Future Prospects: Global Innovations and Future Prospects* (p. 90). IGI Global.

Mauro, P. (1998). Corruption and the Composition of Government Expenditure. *Journal of Public Economics*, *69*(2), 263–279.

McDonald, D., O'Brien, J., Farr, E., & Haaga, D. F. (2010). Pilot Study of Inducing Smoking Cessation Attempts by Activating a Sense of Looming Vulnerability. *Addictive Behaviors*, *35*(6), 599–606.

Mertens, D. . (2005). *Research Methods in Education and Psychology: Integrating Diversity with Quantitative and Qualitative Approaches*. Thousand Oaks: Sage.

Michie, S., Johnston, M., Abraham, C., Lawton, R., Parker, D., & Walker, A. (2005). Making Psychological Theory Useful for Implementing Evidence Based Practice: A Consensus Approach. *Quality and Safety in Health Care*, *14*(1), 26–33.

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and Intervention in Health Related Behavior: A Meta Analytic Review of Protection Motivation Theory. *Journal of Applied Social Psychology*, *30*(1), 106–143.

Miran, I. H., & Rasha, A. E. A. (2013). Investigating e-Banking Service Quality in one of Egypt's Banks: A stakeholder Analysis. *The TQM Journal*, *25*(5), 557–576.

Mitnick, K. D., & Simon, W. L. (2011). *The art of Deception: Controlling the Human Element of Security*. John Wiley & Sons.

Montaño, D., & Kasprzyk, D. (2008). Theory of Reasoned Action, Theory of Planned Behavior, and the Integrated Behavioral Model. In K. Glanz, B. Rimer, & K. Viswanat (Eds.), *Health Behaviour and Health Education* (4th ed., pp. 67–92). San Fransisco, USA: John Wiley & Sons.

Moon, T. K. (1996). The Expectation-Maximization Algorithm. *IEEE Signal Processing Magazine*, *13*(6), 47–60.

Mutarubukwa, A.-A. (2010, January). Tanzania: Concern As Hackers Mess Up Crucial Websites. *The Citizen*. Dar es Salaam, Tanzania.

Mwananchi. (2016, July). Tanzania ipo kwenye mikakati kukabili wizi wa fedha kwa kutumia mitandao. Dar es Salaam, Tanzania.

Myers, M. D. (1997). Qualitative Research In Information Systems. *Management Information Systems Quarterly*, *21*(2), 241–242.

Naing, L., Than, W., & Rusli, B. N. (2006). Practical Issues in Calculating the Sample Size for Prevalence Studies. *Archives of Orofacial Sciences*, *1*, 9–14.

Naser, K., Karbhari, Y., & Zulkifli Mokhtar, M. (2004). Impact of ISO 9000 registration on company performance. *Managerial Auditing Journal*, *19*(4), 509–516.

NBS. (2012). *Employment and Earnings Survey: Analytical Report*. Dar es Salaam, Tanzania.

Nfuka, E. N., Sanga, C., & Mshangi, M. (2014). The Rapid Growth of Cybercrimes Affecting Information Systems in the Global : Is this a Myth or Reality in Tanzania ? *International Journal of Information Security Science*, *3*(2), 182–199.

Ng, B., Kankanhalli, A., & Xu, Y. (2009). Studying Users' Computer Security behavior: A health Belief Perspective. *Decision Support Systems*, *46*(4), 815–825.

Ng, B., & Rahim, M. (2005). A Socio-Behavioral Study of Home Computer Users ' Intention to Practice Security. *Proceedings of the Ninth Pacific Asia Conference on Information Systems*, *2003*, 234–247.

Nguyen, Q. N., & Kim, D. J. (2017). Enforcing Information Security Protection : Risk Propensity and Self-Efficacy Perspectives. In *Proceedings of the 50th Hawaii International Conference on System Sciences* (pp. 4947–4956). Hawaii.

Nungu, A. (2012). Cyber Security in Tanzania: Roles and Responsibilities. In *CyberSecurity Mini-Conference* (pp. 1–3). Dar es Salaam, Tanzania.

O'Rourke, N., & Hatcher, L. (2013). *A Step-by-Step Approach to Using SAS for Factor Analysis and Structural Equation Modeling* (Second Edi). Cary, North Carolina: SAS Institute.

OECD. (2003). Glossary of Statistical Terms. Retrieved March 25, 2017, from https://stats.oecd.org/glossary/detail.asp?ID=742

Ohme, J. (2014). The acceptance of mobile government from a citizens' perspective: Identifying perceived risks and perceived benefits. *Mobile Media & Communication*, *2*(3), 298–317.

Oliveira, D., Rocha, H., Yang, H., Ellis, D., Dommaraju, S., Muradoglu, M., … Ebner, N. (2017). Dissecting Spear Phishing Emails for Older vs Young Adults: On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing. In *Conference on Human Factors in Computing Systems* (pp. 6412–6424). Denver, CO, USA: ACM.

Or, C., & Karsh, B.-T. (2009). A Systematic Review of Patient Acceptance of Consumer Health Information technology. *Journal of the American Medical Informatics Association : JAMIA*, *16*(4), 550–60.

Orbelll, S., Blair, C., & Essex, U. (2001). The Theory of Planned Behavior and Ecstasy Use : Roles for Habit and Perceived Control Over Taking Versus Obtaining Substances. *Journal of Applied Social Psychology*, *31*(1), 31–47.

Oreku, G. S., & Mtenzi, F. J. (2012). A Review of e-Government Initiatives in Tanzania: Challenges and Opportunities. In K. J. Bwalya & S. F. C. Zulu (Eds.), *Handbook of Research on E-Government in Emerging Economies: Adoption, E-Participation, and Legal Frameworks: Adoption, E-Participation, and Legal Frameworks* (pp. 37–70). Hershey, PA: IGI Global.

Orji, R., Vassileva, J., & Mandryk, R. (2012). Towards an Effective Health Interventions Design: An Extension of the Health Belief Model. *Online Journal of Public Health Informatics*, *4*(3).

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying Information Technology in Organizations: Research Approaches and Assumptions. *Information Systems Research*, *2*(1), 1–28.

Osborne, J., & Overbay, A. (2008). Best Practices in Data Cleaning : How Outliers and Fringeliers Can Increase Error Rates and Decrease Precision of Your Results. In *Best Practices in Quantitative Methods* (pp. 205–213). Sage Publications, Inc.

Ouellette, J., & Wood, W. (1998). Habit and Intention in Everyday Life : The Multiple Processes by Which Past Behavior Predicts Future Behavior. *Psychological Bulletin*, *124*(1), 54–74.

Pahnila, S., Siponen, M., & Mahmood, A. (2007a). Employees ' Behavior towards IS Security Policy Compliance. In *Proceedings of the 40th Hawaii International Conference on System Sciences* (pp. 1–10). Honolulu, Hawaii.

Pahnila, S., Siponen, M., & Mahmood, A. (2007b). Which Factors Explain Employees' Adherence to Information Security Policies? An Empirical Study. In *Pacis 2007 Proceedings* (pp. 438–439). Aukland, USA.

Pampaka, M., Hutcheson, G., & Williams, J. (2014). Handling Missing Data: Analysis of a Challenging Data Set Using Multiple Imputation. *International Journal of Research & Method in Education*, *39*(1), 20–37.

Parsian, N., & Dunning, T. (2009). Developing and Validating a Questionnaire to Measure Spirituality: A psychometric Process. *Global Journal of Health Science*, *1*(1), 2–11.

Paulsen, C., & Coulson, T. (2011). Beyond Awareness: Using Business Intelligence to Create a Culture of Information Security. *Communications of the IIMA*, *11*(3), 35–55.

Paulsen, N., Callan, V. J., Ayoko, O., & Saunders, D. (2013). Transformational Leadership and Innovation in an R&D Organization Experiencing Major Change. *Journal of Organizational Change Management*, *26*(3), 595–610.

PCI. (2014). Information Supplement : Best Practices for Implementing a Security Awareness Program. Security Standard Council.

Pedhazur, E. (1982). *Multiple Regressions In Behavioral Research : Explanation and Prediction* (2nd ed.). New York, USA: Holt, Rinehart and Winston.

Pedhazur, E., & Schmelkin, L. P. (2013). *Measurement, Design, and Analysis: An integrated Approach*. New York, USA: Psychology Press.

Penard, T., Poussing, N., Mukoko, B., & Piaptie, G. B. T. (2015). Internet Adoption and Usage Patterns in Africa: Evidence from Cameroon. *Technology in Society*, *42*(1), 71–80.

Peter, J. P. (1981). Construct Validity: A review of Basic Issues and Marketing Practices. *Journal of Marketing Research*, *18*(2), 133–145.

Peterson, R. A., & Kim, Y. (2013). On the Relationship Between Coefficient Alpha and Composite Reliability. *Journal of Applied Psychology*, *98*(1), 194.

Peyman, N., Hidarnia, A., Ghofranipour, F., Kazemnezhad, A., Oakley, D., Khodaee, G., & Aminshokravi, F. (2009). Self-efficacy: Does it Predict the Effectiveness of Contraceptive Use in Iranian Women? *Eastern Mediterranean Health Journal*, *15*(5), 1254–1262.

Pirzadeh, H., Shanian, S., Hamou-lhadj, A., & Alawneh, L. (2013). Stratified Sampling of Execution Traces : Execution Phases Serving as Strata. *Science of Computer Programming*, *78*(8), 1099–1118.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common Method Biases in Behavioral Research: A critical Review of the Literature and Recommended Remedies. *Journal of Applied Psychology*, *88*(5), 879.

Podsakoff, P. M., Mackenzie, S. B., Lee, J., & Podsakoff, N. P. (2003). Common Method Biases in Behavioral Research : A Critical Review of the Literature and Recommended Remedies. *Journal of Applied Psychology*, *88*(5), 879–903.

Podsakoff, P. M., & Organ, D. W. (1986). Self-reports in Organizational Research: Problems and Prospects. *Journal of Management*, *12*(4), 531–544.

Polit, D. F., Beck, C. T., & Owen, S. V. (2007). Is the CVI an Acceptable Indicator of Content Validity? Appraisal and Recommendations. *Research in Nursing & Health*, *30*(4), 459–467.

Pollard, B. (2005). The Rationality of Habitual Actions. In *Proceedings of the Durham-Bergen Philosophy Conference* (pp. 39–50). Bergen, Norway.

Preacher, K. J., & Hayes, A. F. (2008). Asymptotic and Resampling Strategies for Assessing and Comparing Indirect Effects in Multiple Mediator Models. *Behavior Research Methods*, *40*(3), 879–891.

Preston, C. C., & Colman, A. M. (2000). Optimal Number of Response Categories in Rating Scales : Reliability , Validity , Discriminating Power , and Respondent Preferences. *Acta Psychologia*, *104*(1), 1–15.

Pruett, M., Shinnar, R., Toney, B., Llopis, F., & Fox, J. (2009). Explaining Entrepreneurial Intentions of University Students: A Cross-Cultural Study. *International Journal of Entrepreneurial Behavior & Research*, *15*(6), 571–594.

Qing, W. (2016). Computer Network Security and Defense Technology Research. In *Eighth International Conference on Measuring Technology and Mechatronics Automation Computer* (pp. 155–157). Macau, China. http://doi.org/10.1109/ICMTMA.2016.47

Quirk, T. J. (2012). *Excel 2010 for Social Science Statistics: A Guide to Solving Practical Problems*. New York: Springer Science & Business Media.

Rahman, S., & Donahue, S. (2010). Convergence of Corporate and Information Security. *International Journal of Computer Science and Information Security*, *7*(1), 63–68.

Rasmussen, J. (1997). Risk Management in a Dynamic Society: A Modelling Problem. *Safety Science*, *27*(2), 183–213.

Reinartz, W., Haenlein, M., & Henseler, J. (2009). An Empirical Comparison of the Efficacy of Covariance-Based and Variance-Based SEM. *International Journal of Research in Marketing*, *26*(4), 332–344.

Reiser, L. M. (2007). *Health Beliefs and Behaviors of College Women*. University of Pittsburgh, USA.

Reisi, M., Javadzade, S. H., Shahnazi, H., Sharifirad, G., Charkazi, A., & Moodi, M. (2014). Factors Affecting Cigarette Smoking Based on Health Belief Model Structures in Pre-university Students in Isfahan, Iran. *Journal of Education and Health Promotion*, *3*, 23.

Reyns, B. (2013). Online Routines and Identity Theft Victimization. *Journal of Research in Crime and Delinquency*, *50*(2), 216–238.

Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in Information Security: Its Influence on End users' Information Security Practice Behavior. *Computers & Security*, *28*(8), 816–826.

Rhemtulla, M., Brosseau-Liard, P., & Savalei, V. (2012). When Can Categorical Variables be Treated as Continuous? A comparison of Robust Continuous and Categorical SEM Estimation Methods under Suboptimal Conditions. *Psychological Methods*, *17*(3), 354–373.

Rimal, R. N. (2000). Closing the Knowledge-Behavior gap in Health promotion: The mediating role of Self-efficacy. *Health Communication*, *12*(3), 219–237.

RITA. (2016). Birth Registration System. Retrieved September 24, 2016, from http://www.rita.go.tz/page.php?pg=633&lang=en

Rogers, R. (1983). Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation Theory",. In J. Cacioppo & R. Petty (Eds.), *in Social Psychophysiology* (pp. 153–176). New York: Guilford.

Rogers, R., & Prentice-Dunn, S. (1997). Protection Motivation Theory. In *Handbook of Health Behavior Research 1: Personal and Social Determinants* (pp. 113–132). New York: Plenum Press.

Rosenstock, I. M. (1966). Why People Use Health Services. *Milbank Quarterly*, *83*(4), 1–32.

Rosenstock, I. M. (1974). Historical Origins of the Health Belief Model. *Health and Behaviour*, *2*(4), 328–335.

Rosenstock, I. M., Strecher, V. J., & Becker, M. H. (1988). Social Learning Theory and The Health Belief Model. *Health Education & Behavior*, *15*(2), 175–183.

Rumsey, D. J. (2011). *Statistics for Dummies* (2nd Ed). Indianapolis, Indiana, USA: John Wiley & Sons.

Rundall, T. G., & Wheeler, J. R. C. (1979). The Effect of Income on Use of Preventive Care : An Evaluation of Alternative Explanations. *Journal of Health and Social Behavior*, *20*(4), 397–406.

Saba, A., Moneta, E., Nardo, N., & Sinesio, F. (1998). Attitudes , Habit , Sensoryand Liking Expectation As Ofmilk. *Food Quality and Preference*, *9*(l), 31–41.

Saba, A., Vassallo, M., & Turrini, A. (2000). The Role of Attitudes , Intentions and Habit in Predicting Actual Consumption of Fat Containing Foods in Italy. *Europeann Journal of Clinical of Nutrition*, *54*(7), 540–545.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information Security Conscious Care Behaviour Formation in Organizations. *Computers and Security*, *53*, 65–78.

Salleh, K. A., & Janczewski, L. J. (2016). Adoption of Big Data Solutions: A study on its security determinants using Sec-TOE Framework. In *International Conference on Information Resources* (p. 66).

Sasse, M., Ashenden, D., Lawrence, D., Coles-Kemp, L., Flechais, I., & Kearney, P. (2007). *Human Vulnerabilities in Security Systems: White Paper*. *Cyber Security Knowledge Transfer Network (KTN)*. Buenos Aires, Argentina.

Sawe, D. (2007). *Serikali Mtandao: Madhumuni, Matatizo, Mafanikio, na Changamoto*. Dar es Salaam.

Schacter, D. L. (1999). The Seven Sins of Memory: Insights from Psychology and Cognitive Neuroscience. *American Psychologist*, *54*(3), 182.

Schmidt, F. L., & Hunter, J. E. (1996). Measurement Error in Psychological Research: Lessons from 26 Research Scenarios. *Psychological Methods*, *1*(2), 199.

Schmidt, F. L., & Hunter, J. E. (1999). Theory Testing and Measurement Error. *Intelligence*, *27*(3), 183–198.

Schneier, B. (2011). *Secrets and Lies: Digital Security in a Networked World*. Indianapolis, Indiana, USA.

Schumacker, R. E., & Lomax, R. G. (2015). *A Beginner's Guide to Structural Equation Modeling* (3rd ed.). Psychology Press.

Schwarzer, R., & Fuchs, R. (1996). Self-Efficacy and Health Behaviours. *Predicting Health Behaviour: Research and Practice with Social Cognition Models*, 163–196.

Sebescen, N., & Vitak, J. (2017). Securing the Human: Employee Security Vulnerability Risk in Organizational Setting. *Journal of the Association for Information Science and Technology*, *68*(9), 2237–2247.

Semboja, H., Silla, B., & Musuguri, J. (2017). Global Scientific. *Cyber Security Institutional Framework in Tanzania: A Policy Analysis*, *5*(6), 13–28.

Shaaban, H. (2014). *Enhancing Governance of Information Security in Developing Countries: The Case of Zanzibar*. University of Bedfordshire.

Shaaban, H., Conrad, M., & French, T. (2012). State of Information Security in Zanzibar's Public Sector. In IST (Ed.), *IST-Africa*. Dar es Salaam, Tanzania.

Sharafkhani, N., Khorsandi, M., & Shamsi, M. (2014). Low Back Pain Preventive Behaviors Among Nurses Based on the Health Belief Model Constructs. *Sage Open*, *4*(4), 1–7.

Sharma, G. R. K. (2006). *Cyber Livestock Communication And Extension Education*. New Delhi, India: Concept Publishing Company.

Shaw, B. A., & Spokane, L. S. (2008). Examining the Association Between Education Level and Physical Activity Changes During Early Old Age. *Journal of Aging and Health*, *20*(7), 767–787.

Sheeran, P., & Abraham, C. (1996). The Health Belief Model. In M. Conner & P. Norman (Eds.), *Predicting Health Behaviour* (Vol. 2, pp. 29–80). McGraw-Hill Education, UK.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. In *Proceedings of the 28th international conference on Human factors in computing systems - CHI '10* (pp. 373–382). Atlanta,Georgia, USA.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Anti-phishing Phil: The Design and Evaluation of a Game that Teaches People not to Fall for Phish. In *Proceedings of the 3rd symposium on Usable privacy and security* (pp. 88–99). Pittsburgh, PA, USA: ACM.

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, Attitudes, and Intentions: Predicting Initial Adoption of Information Security Behavior. *Computers and Security*, *49*, 177–191.

Siponen, M., Mahmood, M., & Pahnila, S. (2014). Employees' Adherence to Information Security policies: An Exploratory Field Study. *Information and Management*, *51*(2), 217–224.

Siponen, M., Pahnila, S., & Mahmood, A. (2006). Factors Influencing Protection Motivation and IS Security Policy Compliance. In *Innovations in Information Technology* (pp. 1–5). Dubai, Emirates: IEEE.

Sobel, M. E. (1982). Asymptotic Confidence Intervals for Indirect Effects in Structural Equation Models. *Sociological Methodology*, *13*(1982), 290–312.

Srivastava, S., Bhatia, M. S., Rajoura, O. P., Kumari, A., & Sinha, V. K. (2012). A Pilot Study to Calculate the Sample Size for the Prevalence of Aggression in Psychiatric Outpatient Setting. *Delphi Psychiatry Journal*, *15*(2), 359–361.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005a). Analysis of End User Security Behaviors. *Computers & Security*, *24*(2), 124–133.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005b). Analysis of End User Security Behaviors. *Computers and Security*, *24*(2), 124–133.

Steers, R. M., Mowday, R. T., & Shapiro, D. L. (2004). The Future of Work Motivation Theory. *Academy of Management Review*, *29*(3), 379–387.

Steinmetz, G. (2005). Positivism and its Others in the Social Sciences. In G. Steinmetz (Ed.), *The Politics of Method in the Human Sciences: Positivism and Its Epistemological Others* (pp. 1–56). Durham,London, UK: Duke University Press.

Straub, D. W. (1990). Effective IS Security: An Empirical Study. *Information Systems Research*, *1*(3), 255–276.

Strecher, V. J., & Rosenstock, I. M. (1997). The Health Belief Model. In S. Ayers, A. Baum, C. McManus, S. Newman, K. Wallston, J. Weinman, & Robert West (Eds.), *Cambridge Handbook of Psychology, Health and Medicine* (pp. 113–117). Cambridge, UK: Cambridge University Press.

Stroebe, W. (2011). *Social Psychology and Health* (2nd ed.). Buckingham , Philadelphia, USA: Open University Press Buckingham.

Sullivan, L. E. (2009). *The SAGE Glossary of the Social and Behavioral Sciences*. London, UK: Sage.

Sultan, F., Urban, G., Shankar, V., & Bart, I. (2003). *Determinants and role of trust in e-business: a large scale empirical study* (No. 4282–2).

Tamjidyamcholo, A., Baba, M. S. Bin, Tamjid, H., & Gholipour, R. (2013). Information security–Professional perceptions of knowledge-sharing intention under self-efficacy, trust, reciprocity, and shared-language. *Computers & Education*, *68*, 223–232.

Tarimo, C. N., Bakari, J. K., Yngström, L., & Kowalski, S. (2006). A Social-Technical View of ICT Security Issues, Trends, and Challenges: Towards a Culture of ICT Security-The Case of Tanzania. In *Information Security South Africa(ISSA)* (pp. 1–12). Sandton, South Africa.

Taylor, D., Bury, M., Campling, N., Carter, S., Garfied, S., Newbould, J., & Rennie, T. (2007). A Review of the use of the Health Belief Model (HBM), the Theory of Reasoned Action (TRA), the Theory of Planned Behaviour (TPB) and the Trans-Theoretical Model (TTM) to Study and Predict Health Related Behaviour Change.

TCRA. (2012). *Report of the Steering Commitee on Establishment of National Computer Response Team (TZ- CERT) Tanzania*. Dar es Salaam.

Thabane, L., Ma, J., Chu, R., Cheng, J., Ismaila, A., Rios, L. P., … Goldsmith, C. H. (2010). A Tutorial on Pilot Studies: The What, Why and How. *BMC Medical Research Methodology*, *10*(1), 1–10.

Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The Insider Threat to Information Systems and the Effectiveness of ISO17799. *Computers & Security*, *24*(6), 472–484.

Thomson, M. E., & von Solms, R. (1998). Information Security Awareness: Educating your Users Effectively. *Information Management & Computer Security*, *6*(4), 167–173.

Tohidinia, Z., & Mosakhani, M. (2010). Knowledge Sharing Behaviour and its Predictors. *Industrial Management & Data Systems*, *110*(4), 611–631.

Trafimow, D. (2000). Habit as Both a Direct Cause of Intention to Use a Condom as a Moderator of the Attitude-Intention and Subjective Norm-Intention Relations. *Psychology & Health*, *15*(3), 383–393.

Traugutt, M. (2014). *The SAGE Encyclopedia of Social Science Research Methods*. Thousand Oaks: Sage Publications, Inc.

Triandis, H. C. (1979). Values, Attitudes, and Interpersonal Behavior. In *Nebraska Symposium on Motivation*. Nebraska: University of Nebraska Press.

Tversky, A., & Kahneman, D. (1974). Judgment under Uncertainty : Heuristics and Biases. *Science, New Series*, *185*(4157), 1124–1131.

TZCERT. (2017). TZ Cert Services. Retrieved March 8, 2017, from https://www.tzcert.go.tz/services/

UN. (2014). United Nations E-Government Survey 2014: E-Government for the Future We Want. Retrieved August 17, 2015, from http://unpan3.un.org/egovkb/Portals/egovkb/Documents/un/2014-Survey/E-Gov_Complete_Survey-2014.pdf

Urbach, N., & Ahlemann, F. (2010). Structural Equation Modeling in Information Systems Research Using Partial Least Squares. *JITTA: Journal of Information Technology Theory and Application*, *11*(2), 5.

URT. (2006). *Public Service Employment and Pay: the Current State and Trends over the last four years Part I (Main Report)*. Dar es Salaam, Tanzania.

URT. (2013). *Tanzania e-Government Strategy*. Dar es Salaam, Tanzania.

URT. (2016). Online Services. Retrieved September 24, 2016, from http://tanzania.go.tz/onlineservices/index/

Van Teijlingen, E., & Hundley, V. (2001). The Importance of Pilot Studies. *Social Research Update*, (35), 1–4.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information and Management*, *49*(3–4), 190–198.

Verplanken, B., & Aarts, H. (1999). Habit, Attitude, and Planned Behaviour: Is Habit an Empty Construct or an Interesting case of Goal-directed Automaticity? *European Review of Social Psychology*, *10*(1), 101–134.

Verplanken, B., Myrbakk, V., & Rudi, E. (2005). The measurement of habit. In T. Betsch & S. Haberstroh (Eds.), *The routines of decision making* (pp. 231–247). New York, USA: Psychology Press.

Verplanken, B., & Orbell, S. (2003). Reflections on Past Behavior: A Self-Report Index of Habit Strength1. *Journal of Applied Social Psychology*, *33*(6), 1313–1330.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers and Security*, *23*(3), 191–198.

Wall, J. D., Palvia, P., & Lowry, P. B. (2013). Control-related motivations and information security policy compliance: The role of autonomy and efficacy. *Journal of Information Privacy and Security*, *9*(4), 52–79.

Warkentin, M., Johnston, A. ., Walden, E. A., & Straub, D. . (2016). Neural Correlates of Protection Motivation for Secure IT Behaviors: An fMRI Exploration. *Journal of the Association for Information Systems*, *17*(3), 194–215.

Waziri, M. D., & Yonah, Z. O. (2014a). A Secure Maturity Model for Protecting e-Government Services : A Case of Tanzania. *ACSIJ Advances in Computer Science : An International Journal*, *3*(5), 98–106.

Waziri, M. D., & Yonah, Z. O. (2014b). Towards a Secure Maturity Model for Protecting e-Government Services in Tanzania : A Stakeholders View. *ACSIJ Advances in Computer Science : An International Journal*, *3*(6), 29–37.

Weaver, F. M., & Carroll, J. S. (1985). Crime Perceptions in a Natural Setting by Expert and Novice Shoplifters. *Social Psychology Quarterly*, *48*(4), 349–359.

Webb, T. L. (2006). Does Changing Behavioral Intentions Engender Behavior Change ? A Meta-Analysis of the Experimental Evidence. *Psychological Bulletin*, *132*(2), 249–268.

Webb, T. L., & Sheeran, P. (2006). Does Changing Behavioral Intentions Engender Behavior Change? A meta-Analysis of the Experimental Evidence. *Psychological Bulletin*, *132*(2), 249–268.

West, S. G., Finch, J. F., & Curran, P. J. (1995). Structural Equation Models with Nonnormal Variables. In R. H. Hoyle (Ed.), *Structural Equation Modeling: Concepts, Isues, and Applications* (pp. 56–75). Thousand Oaks: Sage Publications, Inc.

White, K. M., Terry, D. J., & Hogg, M. A. (1994). Safer Sex Behavior: The Role of Attitudes, Norms, and Control Factors. *Journal of Applied Social Psychology*, *24*(24), 2164–2192.

Wiersma, U. J. (1992). The effects of Extrinsic Rewards in Intrinsic Motivation: A Meta-Analysis. *Journal of Occupational and Organizational Psychology*, *65*(2), 101–114.

Williams, K. R., & Hawkins, R. (1986). Perceptual Research on General Deterrence: A Critical Review. *Law and Society Review*, *20*(4), 545–572.

Williams, L. J., & Anderson, S. E. (1994). An alternative approach to method effects by using latent-variable models: Applications in organizational behavior research. *Journal of Applied Psychology*, *79*(3), 323.

Wood, W., & Neal, D. (2007). A New Look at Habits and the Habit-Goal Interface. *Psychological Review*, *114*(4), 843.

Woon, I., Tan, G., & Low, R. (2005). A Protection Motivation Theory Approach to Home Wireless Security. In *Proceedings of the Twenty-Sixth International Conference on Information Systems* (pp. 367–380). Las Vegas, USA.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security Lapses and he Omission of Information Security Measures: A threat Control Model and Empirical Test. *Computers in Human Behavior*, *24*, 2799–2816.

Wright, K. B. (2005). Researching Internet Based Populations: Advantages and Disadvantages of Online Survey Research, Online Questionnaire Authoring Software Packages, and Web Survey Services. *Journal of Computer Mediated Communication*, *10*(3).

Yang, C., & Lee, H. (2016). A Study on the Antecedents of Healthcare Information Protection Intention. *Information Systems Frontiers*, *18*(2), 253–263.

Yang, Z., Wang, X., & Su, C. (2006). A Review of Research Methodologies in International Business. *International Business Review*, *15*(6), 601–617.

Yin, J., Karimi, S., Lampert, A., Cameron, M., Robinson, B., & Power, R. (2015). Using social media to enhance emergency situation awareness: In *IJCAI International Joint Conference on Artificial Intelligence* (pp. 4234–4239). IEE.

Ylitalo, J. (2009). *Controlling for Common Method Variance with Partial Least Squares Path Modeling: A Monte Carlo Study*. Helsinki.

Yoon, C. (2011). Theory of Planned Behavior and Ethics Theory in Digital Piracy : An Integrated Model. *Journal of Business Ethics*, (100), 405–417.

Yoon, C., Hwang, J., & Kim, R. (2012). Exploring Factors that Influence Students' Behaviors in Information Security. *Journal of Information Systems Education*, *23*(4), 407–416.

Youn, S. (2009). Determinants of Online Privacy Concern and its Influence on Privacy Protection Behaviors among young Adolescents. *Journal of Consumer Affairs*, *43*(3), 389–418.

Yun, T., & Arriaga, R. I. (2013). A Text Message a Day Keeps the Pulmonologist Away. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 1769–1778). Paris, France: ACM Press.

Zhang, J., Reithel, B., & Li, H. (2009). Impact of Perceived Technical Protection on Security Behaviors. *Information Management & Computer Security*, *17*(4), 330–340.

Zukowski, T., & Brown, I. (2007). Examining the Influence of Demographic Factors on Internet Users' Information Privacy Concerns. In *Proceedings of the 2007 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries* (pp. 197–204). Port Elizabeth, South Africa: ACM.

APPENDICES

Appendix A: List of e- Services

List of e- Services offered by the Government
Register for Taxpayer Identification number (TIN)
EFDMS Public Portal
Register for Payment (E- filling and Online registration payment)
Register for Value added tax (VAT)
Customs licence management
Value added tax (VAT) Return submission
Cargo Tracking and management Services
Artistic Products Registration
Vessel online calls declaration using Harbour View System
Shipping Information
e-Payment System
Registration in Central Admission System (CAS)
Foreign Awards Assessment System (FAAS)
Programmes Management Systems (PMS)
Register for Online Water Bill
Checking your Water Bill
Online loan Application for Higher Education
Register for Membership in Social funds
Retirement Benefit Calculator
Birth Registration Services
Register for Retirement Benefits Mandatory Scheme
Register for Retirement Benefits supplementary Scheme
Online Electric Bills issuing
Crime Reporting

Source : (RITA, 2016; URT, 2016)

Appendix B: Consent forms, Ethical approval and Questionnaires

Appendix B1: A Sample Consent Form

UNIVERSITI TUNKU ABDUL RAHMAN			
Form Title: **VOLUNTEER INFORMATION AND CONSENT FORM**			
Form Number:**FM-IPSR-R&D-057**	Rev No: 2	Effective Date: **12/7/2016**	Page No:**192 of 260**

(PARTICIPATION IN THIS RESEARCH IS VOLUNTARY)

1. Investigators' Name:				**Faculty** : FBF	
Title of research project	:				
Purpose of study					
Procedure	:				
Risk and Discomfort					
Benefit Payment Alternatives					
Contact Person					
Note: 1. All volunteers involved in this study will not be covered by insurance *2. Contact person must be the principal investigator/supervisor*					
2. Particulars of Volunteer (Volunteer Identifier/Label) *(Please use separate form if more than one volunteer)*					
Full Name	:				
Chinese character *(if applicable)*	:				
New Identity Card/	:				
Passport No.	:				
Gender					
Contact No.	:				

Email	:	

3. Voluntary participation

You understand that participation in this study is voluntary and that if you decide not to participate, you will experience no penalty or loss of benefits to which you would otherwise be entitled. If you decide to participate, you may subsequently change your mind about being in the study and may stop participating at any time. You understand that you must inform the principal investigator of your decision immediately.

4. Available Medical Treatment

If you are injured during your participation or in the course of the study or whether or not as a direct result of this study, UTAR will not be liable for any loss or damage or compensation or absorb the costs of medical treatment. However, assistance will be provided to you in obtaining emergency medical treatment.

5. Confidentiality

All information, samples and specimens you have supplied will be kept confidential by the principal investigator and the research team and will not be made available to the public unless disclosure is required by law.

6. Disclosure

Data, samples and specimens obtained from this study will not identify you individually. The data, samples and specimens may be given to the sponsor and/or regulatory authorities and may be published or be reused for research purposes not detailed within this consent form. However, your identity will not be disclosed. The original records will be reviewed by the principal investigator and the research team, the UTAR Scientific and Ethical Review Committee, the sponsor and regulatory authorities for the purpose of verifying research procedures and/or data.

By signing this consent form, you authorise the record review, publication and re-utilisation of data, information and sample storage and data transfer as described above

7. Declaration

I have read or had the information above read to me, in the language understandable to me. The above content has been fully explained to me.

I have asked all questions that I need to know about the study and this form. All my questions have been answered. I have read, or have had read to me, all pages of this consent form and the risks described. I voluntarily consent and offer to take part in this study. By signing this consent form, I certify that all information I have given, including my medical history, is true and correct to the best of my knowledge. **I will not hold UTAR or the research team responsible for any consequences and/or liability whatsoever arising from my participation in this study.**

8. Consent

If you wish to participate in this study, please sign below.

_____ _____

Signature of Volunteer IC/Passport No.

_____ _____

Name of Volunteer Date

_____ _____

Signature of witness IC/Passport No.

_____ _____

Name of witness Date

9. Statement of Principal Investigator/Supervisor

I have fully explained to the volunteer taking part in this study what he/she can expect by virtue of his / her participation. The volunteer who is giving consent to take part in this study

- Understands the language that I have used.
- Reads well enough to understand this form, or is able to hear and understand the contents of the form when read to him or her.
- Is of the age of majority of 18 or above.

To the best of my knowledge, when the volunteer signed this form, he or she understands:

- That taking part in the study is voluntary.
- What the study is about.
- What needs to be done?
- What are the potential benefits?
- What are the known risks?

A copy of this consent form has been given to the volunteer.

_____
_____

Name of Principal Investigator/Supervisor IC/Passport No.

_____ _____

Signature of Principal Investigator/Supervisor Date

Note: *1. The principal investigator/supervisor conducting the informed consent process, must sign* ***and*** *date form* ***at the same time as the volunteer****.*

Appendix B2: Ethical Approval Letter

UNIVERSITI TUNKU ABDUL RAHMAN
Wholly Owned by UTAR Education Foundation (Company No. 578227-M)

Re: U/SERC/49/2016

12 July 2016

Dr Chong Yee Lee
Department of Marketing
Faculty of Business and Finance
Universiti Tunku Abdul Rahman
Jalan Universiti, Bandar Baru Barat
31900 Kampar
Perak

Dear Dr Chong,

Ethical Approval For Research Project/Protocol

We refer to your application dated 6 June 2016 for ethical approval for your research project (PhD candidate's project) and are pleased to inform you that your application has been approved under expedited review.

The details of your research project are as follows:

Research Title	Analysis of Protective Information Security Behaviour Among Government Employees in Tanzania Using the Health Belief Model
Investigator(s)	Dr Chong Yee Lee (PI) Mr Daniel Ntabagi Koloseni (UTAR Postgraduate Student)
Research Area	Social Sciences
Research Location	Dar Es Salaam, Tanzania
No of Participants	384 participants (Age: 18 and above)
Research Costs	Self-funded
Approval Validity	12 July 2016 - 11 July 2017

The conduct of this research is subject to the following:

(1) The participants' informed consent be obtained prior to the commencement of the research,

(2) Confidentiality of participants' personal data must be maintained; and

(3) Compliance with procedures set out in related policies of UTAR such as the UTAR Research Ethics and Code of Conduct, Code of Practice for Research Involving Humans and other related policies/guidelines.

Should you collect personal data of participants in your study, please have the participants sign the attached Personal Data Protection Statement for your records.

The University wishes you all the best in your research.

Thank you.

Yours sincerely,

Professor Ir Dr Lee Sze Wei
Chairman
UTAR Scientific and Ethical Review Committee

c.c Dean, Faculty of Business and Finance
Director, Institute of Postgraduate Studies and Research

Appendix B3: Pre- Test Questionnaire for Refinement

COVER LETTER

Daniel Koloseni
Universiti Tunku Abdul Rahman
Kampar Campus, Malaysia

Dear Prof/Assoc. Prof/Dr.

I am currently doing a research on the "**The Practice of Information Security: An Analysis Of Government Employees in Tanzania Using the Health Belief Model**. This study is conducted as part of my PhD studies at Universiti Tunku Abdul Rahman, Malaysia. I have managed to prepare an instrument adapted from previous studies to measure the construct of interest.

The current stage is to *pre-test the* items to establish whether each item was clearly presented, whether appropriate vocabulary or terms have been used, whether there is no ambiguous question – question with more than one interpretation, and double questions- two questions to which a respondent is asked to provide a single answer and whether questionnaire items match their operational definition. I would be grateful if you could spend some time to read through the items and comment on the attached questionnaire.

Thank you very much in advance for allocating your valuable time to comment on my questionnaire.
Yours sincerely,

Daniel Ntabagi Koloseni (Researcher)
PhD Student
Mobile number: + 255767 619 998
Email: dkoloseni@gmail.com

QUESTIONNAIRE

REF: THE PRACTICE OF INFORMATION SECURITY: AN ANALYSIS OF GOVERNMENT EMPLOYEES IN TANZANIA USING THE HEALTH BELIEF MODEL

Dear Sir/ Madam,

I am undertaking a research on "**The Practice of Information Security: An Analysis Of Government Employees in Tanzania Using the Health Belief Model**". This study is conducted as part of my PhD studies at Universiti Tunku Abdul Rahman, Malaysia.
I would greatly appreciate if you could complete this questionnaire based on your honest opinion. There is no right or wrong answer. Please make a full effort to answer each question.
I would like to assure you that all answers will be kept strictly **confidential** and will be used only for this research. If you have any inquiries or problem in answering the questionnaire, please contact the name of researcher below.
Thank you very much for your kind assistance.
Yours Sincerely

Daniel Ntabagi Koloseni (Researcher)
PhD Student
Mobile number: + 255767 619 998

PART A: Respondent's Demographics

Instructions**: Please tick ONE appropriate answer**.

1. Please indicate your gender.

☐ Male ☐ Female

2. In which age range do you fall in?

☐ 18- 45 years ☐ 46 years and above

3. Please indicate your level of Education.

☐ O'level
☐ A'level
☐ Diploma or Equivalent
☐ Degree or Equivalent
☐ Master's Degree
☐ Doctorate Degree

4. In which type of organisation are you working in?

☐ Ministry
☐ Authority
☐ Social Fund
☐ Board
☐ Commission

PART B: Perception on Information Security Behaviour

Operational definition	Questionnaire items	Comments
Perceived severity Consequences an individual may experience as a result of security attack to the organisation and information resources.	1. If my computer is infected by malicious software such as virus as a result of opening suspicious, untrusted and unsecure websites or email attachment, my daily work could be negatively affected.	
	2. It would cause a serious problem to me if the organisational data that is stored in my computer were stolen/ destroyed by malicious software	

Operational definition	Questionnaire items	Comments
	3. I would be in trouble if my personal identifiable data such as biological traits were stolen by malicious software	
	4. My personal and organisation data that are stored in my computer could be misused by cyber criminals via malicious software	
	5. My personal and organisation data that are stored in my computer could be given to third parties without my knowledge via malicious software	
	6. The invasion of malicious software could make my computer's operation become slower	
	7. The invasion of malicious software could crash my computer's system from time to time	
	8. The invasion of malicious software could make some of my computer programs become difficult to use	
Operational definition	**Questionnaire items**	**Comments**
Perceived susceptibility Employee's belief with regard to vulnerability of an organization to security threats	9. My computer may be infected by malicious software such as computer virus	
	10. It is possible that the cyber criminals could hack or steal the organisation data or information that is stored in my computer	
	11. The data and or application programs which are stored in and or run by my computer could be undermined or damaged by malicious software such as computer virus	
	12. Chances of allowing the malicious software to attack my computer could be high if I	

Operational definition	Questionnaire items	Comments
	open and or use suspicious email or e-attachment	
Perceived benefit Employee's belief on the advantages that could be gained from executing information security actions.	13. Checking whether the suspicious email/ website is NOT from a fraudulent or scammed source is an effective way to prevent malicious software from invading my computer	
	14. Checking whether the file name of a suspicious website/ email/ e-attachment is NOT from a fraudulent or scammed source is an effective way to prevent malicious software from invading my computer.	
	15. If I can prevent malicious software from invading my computer, my work's productivity will improve	
Operational definition	**Questionnaire items**	**Comments**
Perceived barriers Refers to actions that inhibit an individual to perform information security action.	16. It would be complicated for me to check whether the suspicious website or email is from trusted source	
	17. It would be time-consuming to me to check whether the suspicious website or email is from trusted source	
	18. To check whether the suspicious website or email is from trusted source, I may need to put in a considerable investment of some effort other than time	
	19. It is inconvenient to me to check the source of suspected filename or web address before opening the website or emails.	

Operational definition	Questionnaire items	Comments
Cues to action Include factors that can trigger an action towards appropriate information security behaviour.	20. If I read articles on newspaper or magazine or organisation's newsletter about computer vulnerability, I would be more concerned about my computer's chances of being attacked by malicious software	
	21. If I received a notice from a software developer about my computer's system security, I would be more conscious in handling my computer from being attacked	
	22. If a work mate have told me about his/her recent experience of a spyware, I would be more conscious in handling my computer from being attacked	
	23. If I receive reminders from my organisation about security attacks, I would be more cautious in handling my computer from being attacked.	
Operational definition	**Questionnaire items**	**Comments**
Self- efficacy Employee's ability and confidence to perform information security behaviour. Higher ability and confidence may motivate an employee to practice protective information security behaviour.	24. I feel confident that I would be able to identify the suspicious, untrusted and unsecure websites without putting in much effort	
	25. I know where and how to find the information that I need if I encounter difficulty in identifying suspicious, untrusted and unsecure websites or emails	
	26. I have the necessary knowledge and ability to protect my personal and organisation data from external threats	
	27. I can identify a suspicious, untrusted and unsecure sites or email correctly without putting in much effort	

Operational definition	Questionnaire items	Comments
Operational definition	**Questionnaire items**	**Comments**
Security habit This construct refers to security actions that are performed by an employee unconsciously or automatically or without thinking to protect organisation information against security threats	28. I have a habit to remove malicious software once it is detected	
	29. It is norm for me to check suspicious, untrusted, and unsecure websites/ emails before accessing them	
	30. It is my habit to remove malicious software periodically	
	31. Checking whether a suspicious, untrusted and unsecure websites is originated from genuine source is something that I would do without being reminded to do so.	
	32. Checking whether a suspicious, untrusted and unsecure websites or emails is not from fraudulent source is part of my daily routine	
	33. Checking a suspicious, untrusted and unsecure websites or emails before accessing them is something that I feel weird if do not do it	
Operational definition	**Questionnaire items**	**Comments**
Behaviour Intention This construct refers to employee's intention to practice protective information security behaviour.	34. I will check the suspicious, untrusted and unsecure websites before accessing any external software programme or email	
	35. I will take other precautions actions such as not to use personal modems and personal external data storages on the computer that is storing organisation data.	
	36. I will never open suspicious, untrusted and unsecure websites on my computer	
	37. I will continue to check any suspicious, untrusted and unsecure websites emails that	

Operational definition	Questionnaire items	Comments
	could attract my attention before accessing them	
	38. I am certain that I would check the suspicious, untrusted and unsecure websites before accessing them	
Operational definition	**Questionnaire items**	**Comments**
Behaviour This construct refers to actual practice of information security behaviour by an employee	39. I check for the suspicious, untrusted and unsecure websites or emails ensure that the websites or emails were not from fraudulent sources	
	40. Sometimes, I don't check the suspicious, untrusted and unsecure sites if it affects my performance or productivity	
	41. I check the suspicious, untrusted and unsecure websites or emails ONLY when it is convenient for me to do so	
	42. When I am busy, I don't check whether the suspicious websites/ emails were from fraudulent or scammed source	

Appendix B4: Pre- Test Questionnaire for Rating

COVER LETTER

Daniel Ntabagi Koloseni
Universiti Tunku Abdul Rahman
Kampar Campus, Malaysia

Dear Prof/Assoc. Prof/Dr.

I am currently doing a research on the "**The Practice of Information Security: An Analysis Of Government Employees in Tanzania Using the Health Belief Model**". This study is conducted as part of my PhD studies at Universiti Tunku Abdul Rahman, Malaysia. I have managed to prepare an instrument adapted from previous studies to measure the construct of interest.

The current stage is to pre-test the items to establish whether each item is appropriate to be used in this study
I would be grateful if you could spend some time to read through the items and rate the items as "not relevant", "somewhat relevant", "relevant" or "highly relevant".

Thank you very much in advance for allocating your valuable time to comment on my questionnaire.
Yours sincerely,

Daniel Ntabagi Koloseni (Researcher)
PhD Student
Mobile number: + 255767 619 998
Email: dkoloseni@gmail.com

QUESTIONNAIRE

REF: THE PRACTICE OF INFORMATION SECURITY: AN ANALYSIS OF GOVERNMENT EMPLOYEES IN TANZANIA USING THE HEALTH BELIEF MODEL

Dear Sir/ Madam,

I am undertaking a research on "**The Practice of Information Security: An Analysis Of Government Employees in Tanzania Using the Health Belief Model**". This study is conducted as part of my PhD studies at Universiti Tunku Abdul Rahman, Malaysia.

I would greatly appreciate if you could complete this questionnaire based on your honest opinion. There is no right or wrong answer. Please make a full effort to answer each question.

I would like to assure you that all answers will be kept strictly **confidential** and will be used only for this research. If you have any inquiries or problem in answering the questionnaire, please contact the name of researcher below.
Thank you very much for your kind assistance.

Yours Sincerely

Daniel Ntabagi Koloseni (Researcher)
PhD Student
Mobile number: + 255767 619 998

PART A: Respondent's Demographics

Instructions**: Please tick ONE appropriate answer**.

58. Please indicate your gender.

☐ Male ☐ Female

59. In which age range do you fall in?

☐ 18- 45 years ☐ 46 years and above

60. Please indicate your level of Education.

☐ O'level
☐ A'level
☐ Diploma or Equivalent
☐ Degree or Equivalent
☐ Master's Degree
☐ Doctorate Degree

61. In which type of organisation are you working in?

☐ Ministry
☐ Authority
☐ Social Fund
☐ Board
☐ Commission
☐ Government Companies

PART B: Perception on Information Security Behaviour

For each of the statements, please circle ONLY ONE (1) number using the agreement-disagreement scale which you best reflect relevancy of the item in this study.

Operational definition	**Questionnaire items**	Not relevant	somewhat relevant	Relevant	Highly relevant
Perceived severity Consequences an individual may experience as a result of security attack	1. If my computer is infected by malicious software such as virus as a result of opening suspicious, untrusted and unsecure websites or email attachment, my daily work could be negatively affected.	1	2	3	4
	2. It would cause a serious	1	2	3	4

Operational definition	Questionnaire items	Not relevant	somewhat relevant	Relevant	Highly relevant
to the organisation and information resources.	problem to me if the organisational data that is stored in my computer were stolen/ destroyed by malicious software				
	3. I would be in trouble if my personal identifiable data such as biological traits is stolen by malicious software	1	2	3	4
	4. My personal and organisation data that are stored in my computer could be misused by cyber criminals via malicious software	1	2	3	4
	5. My personal and organisation data that are stored in my computer could be sent to third parties without my knowledge via malicious software	1	2	3	4
	6. The invasion of malicious software could make my computer's operation become slower	1	2	3	4
	7. The invasion of malicious software could crash my computer's system from time to time	1	2	3	4
	8. The invasion of malicious software could make some of my computer programs become difficult to use	1	2	3	4
Operational definition	**Questionnaire items**	Not relevant	somewhat relevant	Relevant	Highly relevant
Perceived susceptibility Employee's belief with regard to vulnerability of an organization to security	9. My computer may be infected by malicious software such as computer virus	1	2	3	4
	10. It is possible that the cyber criminals could hack or steal the organisation data or information that is stored in my computer	1	2	3	4
	11. The data and or application	1	2	3	4

Operational definition	Questionnaire items	Not relevant	somewhat relevant	Relevant	Highly relevant
threats	programs which are stored in and or run by my computer could be undermined or damaged by malicious software such as computer virus				
	12. Chances of allowing the malicious software to attack my computer could be high if I open and or use suspicious email or e-attachment	1	2	3	4
Operational definition	**Questionnaire items**	Not relevant	somewha t relevant	Relevant	Highly relevant
Perceived benefit Employee's belief on the advantages that could be gained from executing information security actions.	13. Checking whether the suspicious email/ website is NOT from a fraudulent or scammed source is an effective way to prevent malicious software from invading my computer	1	2	3	4
	14. Checking whether the file name of a suspicious website/ email/ email attachment is NOT from a fraudulent or scammed source is an effective way to prevent malicious software from invading my computer.	1	2	3	4
	15. If I can prevent malicious software from invading my computer, my work's productivity will improve	1	2	3	4
Operational definition	**Questionnaire items**	Not relevant	somewhat relevant	Relevant	Highly relevant
Perceived barriers Refers to actions	16. It would be complicated for me to check whether the suspicious website or email is from trusted source	1	2	3	4

Operational definition	Questionnaire items	Not relevant	somewhat relevant	Relevant	Highly relevant
that inhibit an individual to perform information security action.	17. It would be time-consuming to me to check whether the suspicious website or email is from trusted source	1	2	3	4
	18. To check whether the suspicious website or email is from trusted source, I may need to put in a considerable investment of some effort other than time	1	2	3	4
	19. It is inconvenient to me to check the source of suspected filename or web address before opening the website or emails.	1	2	3	4
Operational definition	**Questionnaire items**	Not relevant	somewhat relevant	Relevant	Highly relevant
Cues to action Include factors that can trigger an action towards appropriate information security behaviour.	20. If I read articles on newspaper or magazine or organisation's newsletter about computer vulnerability, I would be more concerned about my computer's chances of being attacked by malicious software	1	2	3	4
	21. If I received a notice from a software developer about my computer's system security, I would be more conscious in handling my computer from being attacked	1	2	3	4
	22. If a work mate have told me about his/her recent experience of a spyware, I would be more conscious in handling my computer from being attacked	1	2	3	4
	23. If I receive reminders from my organisation about security attacks, I would be more cautious in handling my computer from being attacked	1	2	3	4

Operational definition	Questionnaire items	Not relevant	somewhat relevant	Relevant	Highly relevant
Operational definition	**Questionnaire items**	Not relevant	somewhat relevant	Relevant	Highly relevant
Self- efficacy Employee's ability and confidence to perform information security behaviour. Higher ability and confidence may motivate an employee to practice protective information security behaviour.	24. I feel confident that I would be able to identify the suspicious, untrusted and unsecure websites without putting in much effort	1	2	3	4
	25. I know where and how to find the information that I need if I encounter difficulty in identifying suspicious, untrusted and unsecure websites or emails.	1	2	3	4
	26. I have the necessary knowledge and ability to protect my personal and organisation data from external threats	1	2	3	4
	27. I can identify a suspicious, untrusted and unsecure sites or email correctly without putting in much effort	1	2	3	4
Operational definition	**Questionnaire items**	Not relevant	somewhat relevant	Relevant	Highly relevant
Security habit This construct refers to security actions that are performed by an employee unconsciously or automatically or without thinking to protect organisation information against security	28. I have a habit to remove malicious software once it is detected	1	2	3	4
	29. It is my habit to remove malicious software periodically	1	2	3	4
	30. It is norm for me to check suspicious, untrusted, and unsecure websites/ emails before accessing them	1	2	3	4
	31. Checking whether a suspicious, untrusted and unsecure websites is originated from genuine source is	1	2	3	4

Operational definition	Questionnaire items	Not relevant	somewhat relevant	Relevant	Highly relevant
threats	something that I would do without being reminded to do so.				
	32. Checking whether a suspicious, untrusted and unsecure websites or emails is not from fraudulent source is part of my daily routine	1	2	3	4
	33. Checking a suspicious, untrusted and unsecure websites or emails before accessing them is something that I feel weird if do not do it	1	2	3	4
Operational definition	**Questionnaire items**	Not relevant	somewhat relevant	Relevant	Highly relevant
Behaviour Intention This construct refers to employee's intention to practice protective information security behaviour.	34. I will check the suspicious, untrusted and unsecure websites before accessing any external software programme or email	1	2	3	4
	35. I will take other precautions such as not to use personal modems and personal external data storages on the computer that is storing organisation data.	1	2	3	4
	36. I will never open suspicious, untrusted and unsecure websites on my computer	1	2	3	4
	37. I will continue to check any suspicious, untrusted and unsecure websites emails that could attract my attention before accessing them	1	2	3	4
	38. I am certain that I would check the suspicious, untrusted and unsecure websites before accessing them	1	2	3	4

Operational definition	Questionnaire items	Not relevant	somewhat relevant	Relevant	Highly relevant
Operational definition	**Questionnaire items**	Not relevant	somewhat relevant	Relevant	Highly relevant
Behaviour This construct refers to actual practice of information security behaviour by an employee	39. I check for the suspicious, untrusted and unsecure websites or emails ensure that the websites or emails were not from fraudulent sources	1	2	3	4
	40. Sometimes, I don't check the suspicious, untrusted and unsecure sites if doing so affects my performance or productivity	1	2	3	4
	41. I only check the suspicious, untrusted and unsecure websites or emails when it is convenient for me to do so	1	2	3	4
	42. When I am busy, I don't check whether the suspicious websites/ emails were from fraudulent or scammed source	1	2	3	4

Appendix B5: Pilot Study Questionnaire

QUESTIONNAIRE

REF: THE PRACTICE OF INFORMATION SECURITY: AN ANALYSIS OF GOVERNMENT EMPLOYEES IN TANZANIA USING THE HEALTH BELIEF MODEL

Dear Sir/ Madam,

I am undertaking a pilot study on "**The Practice of Information Security: an Analysis of Government Employees in Tanzania Using the Health Belief Model**".

I would greatly appreciate if you could complete this questionnaire based on your honest opinion. There is no right or wrong answer. Please make a full effort to answer each question as directed.
I would like to assure you that all answers will be kept strictly **confidential** and will be used only for this research. If you have any inquiries or problem in answering the questionnaire, please contact the researcher using the information provided below.

Thank you very much for your kind assistance.

Yours Sincerely

Daniel Ntabagi Koloseni (Researcher)
The Institute of Finance Management
Mobile number: + 255767 619 998
Email: dkoloseni@gmail.com

PART A: Respondent's Demographics

Instructions**: Please tick ONE appropriate answer**.

1. Please indicate your gender.

☐ Male ☐ Female

2. In which age range do you fall in?

☐ 18- 45 years ☐ 46 years and above

3. Please indicate your level of Education.

☐ O'level
☐ A'level
☐ Diploma or Equivalent
☐ Degree or Equivalent
☐ Master's Degree
☐ Doctorate Degree

4. In which type of organisation are you working in?

☐ Ministry
☐ Authority
☐ Social Fund
☐ Board
☐ Commission
☐ Government Companies

PART B: Perceptions on Information Security Behaviour

For each of the statements, in the questionnaire items list, please circle ONLY ONE (1) number using the agreement-disagreement scale which you feel best describes your behaviour.

S/No	Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1.	If my computer is infected by malicious software such as virus as a result of opening suspicious, untrusted and unsecure websites or email attachment, my daily work could be negatively affected.	1	2	3	4	5
2.	It would cause a serious problem to me if the organisational data that is stored in my	1	2	3	4	5

S/No	Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
	computer is stolen/ destroyed by malicious software.					
3.	I would be in trouble if my personal identifiable data such as biological traits, is stolen by malicious software.	1	2	3	4	5
4.	My personal and organisation data that are stored in my computer could be misused by cyber criminals using the malicious software.	1	2	3	4	5
5.	My personal and organisation data that are stored in my computer could be sent to third parties without my knowledge using the malicious software.	1	2	3	4	5
6.	The invasion of malicious software could make my computer's operation become slower.	1	2	3	4	5
7.	The invasion of malicious software could crash my computer's system from time to time	1	2	3	4	5
8.	The invasion of malicious software could make some of my computer programs become difficult to use.	1	2	3	4	5
9.	My computer may be infected by malicious software such as computer virus.	1	2	3	4	5
10.	It is possible that the cyber criminals could hack or steal the organisation's data or information that is stored in my computer	1	2	3	4	5
11.	The data and or application programs which are stored in and or run by my computer could be undermined or damaged by malicious software such as computer virus.	1	2	3	4	5
12.	Chances of allowing the malicious software to attack my computer could be high if I open and or use suspicious email or email attachments.	1	2	3	4	5
13.	Checking whether the suspicious email or website is NOT from a fraudulent or scammed source is an effective way to prevent malicious software from invading my computer.	1	2	3	4	5
14.	Checking whether the file name of a suspicious website, email or an email attachment is NOT from a fraudulent or scammed source is an effective way to prevent malicious software from invading	1	2	3	4	5

S/No	Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
	my computer.					
15.	If I can prevent malicious software from invading my computer, my work's productivity will improve.	1	2	3	4	5
16.	It would be complicated for me to check whether the suspicious website or email is from trusted source.	1	2	3	4	5
17.	It would be time-consuming for me to check whether the suspicious website or email is from trusted source.	1	2	3	4	5
18.	To check whether the suspicious website or email is from trusted source, I may need to put in considerable investment of some effort other than time	1	2	3	4	5
19.	It is inconvenient to me for to check the source of suspected filename or web address before opening the website or emails.	1	2	3	4	5
20.	If I read articles on newspaper or magazine or organisation's newsletter about computer vulnerability, I would be more concerned about my computer's chances of being attacked by malicious software.	1	2	3	4	5
21.	If I received a notice from a software developer about my computer's system security, I would be more conscious in handling my computer from being attacked.	1	2	3	4	5
22.	If a work mate has told me about his or her recent experience of a spyware, I would be more conscious in handling my computer from being attacked.	1	2	3	4	5
23.	If I receive reminders from my organisation about security attacks, I would be more cautious in handling my computer from being attacked.	1	2	3	4	5
24.	I feel confident that I would be able to identify the suspicious, untrusted and unsecure websites without putting in much effort.	1	2	3	4	5
25.	I know where and how to find the information that I need if I encounter difficulty in identifying suspicious, untrusted and unsecure websites or emails.	1	2	3	4	5
26.	I have the necessary knowledge and ability to protect my personal and organisation data from external threats.	1	2	3	4	5

S/No	Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
27.	I can identify a suspicious, untrusted and unsecure websites or emails correctly without putting in much effort.	1	2	3	4	5
28.	I have a habit of removing malicious software once it is detected.	1	2	3	4	5
29.	It is my habit to remove malicious software periodically.	1	2	3	4	5
30.	It is a norm to me to check for suspicious, untrusted and unsecure websites or emails before accessing them.	1	2	3	4	5
31.	Checking whether a suspicious, untrusted and unsecure websites is originated from genuine source is something that I would do without being reminded to do so.	1	2	3	4	5
32.	Checking whether a suspicious, untrusted and unsecure websites or emails are not from fraudulent source is part of my daily routine.	1	2	3	4	5
33.	Checking a suspicious, untrusted and unsecure websites or emails before accessing them is something that I feel weird if I do not do it.	1	2	3	4	5
34.	I will check the suspicious, untrusted and unsecure websites before accessing any external software programme or email.	1	2	3	4	5
35.	I will never open suspicious, untrusted and unsecure websites on my computer.	1	2	3	4	5
36.	I will continue to check any suspicious, untrusted and unsecure websites or emails that could attract my attention before accessing them.	1	2	3	4	5
37.	I am certain that I would check the suspicious, untrusted and unsecure websites before accessing them.	1	2	3	4	5
38.	I check for the suspicious, untrusted and unsecure websites or emails to ensure that the websites or emails were not from fraudulent sources.	1	2	3	4	5
39.	Sometimes, I don’t check for suspicious, untrusted and unsecure websites if doing so affects my performance or productivity.	1	2	3	4	5
40.	I only check for the suspicious, untrusted and unsecure websites or emails when it is convenient for me to do so.	1	2	3	4	5

S/No	Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
41.	When I am busy, I don't check whether the websites or emails I receive were from fraudulent or scammed source.	1	2	3	4	5

Thank you for your assistance!

Appendix B6: Main Study Questionnaire

QUESTIONNAIRE

REF: THE PRACTICE OF INFORMATION SECURITY: AN ANALYSIS OF GOVERNMENT EMPLOYEES IN TANZANIA USING THE HEALTH BELIEF MODEL

Dear Sir/ Madam,

I am undertaking a study on "**The Practice of Information Security: an Analysis of Government Employees in Tanzania Using the Health Belief Model**". I would greatly appreciate if you could complete this questionnaire based on your honest opinion. There is no right or wrong answer. Please make a full effort to answer each question as directed.
I would like to assure you that all answers will be kept strictly **confidential** and will be used only for this research. If you have any inquiries or problem in answering the questionnaire, please contact the researcher using the information provided below.

Thank you very much for your kind assistance.

Yours Sincerely

Daniel Ntabagi Koloseni (Researcher)
The Institute of Finance Management
Mobile number: + 255767 619 998
Email: dkoloseni@gmail.com

PART A: Respondent's Demographics

Instructions**: Please tick ONE appropriate answer**.

5. Please indicate your gender.

☐ Male ☐ Female

6. In which age range do you fall in?

☐ 18- 45 years ☐ 46 years and above

7. Please indicate your level of Education.

☐ O'level
☐ A'level
☐ Diploma or Equivalent
☐ Degree or Equivalent
☐ Master's Degree
☐ Doctorate Degree

8. In which type of organisation are you working in?

☐ Ministry
☐ Authority
☐ Social Fund
☐ Board
☐ Commission
☐ Government Companies

PART B: Perceptions on Information Security Behaviour

For each of the statements, in the questionnaire items list, please circle ONLY ONE (1) number using the agreement-disagreement scale which you feel best describes your behaviour.

No	Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1.	If my computer is infected by malicious software such as virus as a result of opening suspicious, untrusted and unsecure websites or email	1	2	3	4	5

No	Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
	attachment, my daily work could be negatively affected.					
2.	It would cause a serious problem to me if the organisational data that is stored in my computer is stolen/ destroyed by malicious software.	1	2	3	4	5
3.	I would be in trouble if my personal identifiable data such as biological traits, is stolen by malicious software.	1	2	3	4	5
4.	My personal and organisation data that are stored in my computer could be misused by cyber criminals using the malicious software.	1	2	3	4	5
5.	My computer may be infected by malicious software such as computer virus.	1	2	3	4	5
6	It is possible that the cyber criminals could hack or steal the organisation's data or information that is stored in my computer	1	2	3	4	5
7	The data and or application programs which are stored in and or run by my computer could be undermined or damaged by malicious software such as computer virus.	1	2	3	4	5
8	Chances of allowing the malicious software to attack my computer could be high if I open and or use suspicious email or email attachments.	1	2	3	4	5
9	Checking whether the suspicious email or website is NOT from a fraudulent or scammed source is an effective way to prevent malicious software from invading my computer.	1	2	3	4	5
10	Checking whether the file name of a suspicious website, email or an email attachment is NOT from a fraudulent or scammed source is an effective way to prevent malicious software from invading my computer.	1	2	3	4	5
11	If I can prevent malicious software from invading my computer, my work's productivity will improve.	1	2	3	4	5
12	It would be complicated for me to check whether the suspicious website or email is from trusted source.	1	2	3	4	5
13	It would be time-consuming for me to check whether the suspicious website or email is from trusted source.	1	2	3	4	5
14	To check whether the suspicious website or email is from trusted source, I may need to put in considerable investment of some effort other	1	2	3	4	5

No	Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
	than time					
15	It is inconvenient to me for to check the source of suspected filename or web address before opening the website or emails.	1	2	3	4	5
16	If I read articles on newspaper or magazine or organisation's newsletter about computer vulnerability, I would be more concerned about my computer's chances of being attacked by malicious software.	1	2	3	4	5
17	If I received a notice from a software developer about my computer's system security, I would be more conscious in handling my computer from being attacked.	1	2	3	4	5
18	If a work mate has told me about his or her recent experience of a spyware, I would be more conscious in handling my computer from being attacked.	1	2	3	4	5
19	If I receive reminders from my organisation about security attacks, I would be more cautious in handling my computer from being attacked.	1	2	3	4	5
20	I feel confident that I would be able to identify the suspicious, untrusted and unsecure websites without putting in much effort.	1	2	3	4	5
21	I know where and how to find the information that I need if I encounter difficulty in identifying suspicious, untrusted and unsecure websites or emails.	1	2	3	4	5
22	I have the necessary knowledge and ability to protect my personal and organisation data from external threats.	1	2	3	4	5
23	I can identify a suspicious, untrusted and unsecure websites or emails correctly without putting in much effort.	1	2	3	4	5
24	I have a habit of removing malicious software once it is detected.	1	2	3	4	5
25	It is my habit to remove malicious software periodically.	1	2	3	4	5
26	It is a norm to me to check for suspicious, untrusted and unsecure websites or emails before accessing them.	1	2	3	4	5
27	Checking whether a suspicious, untrusted and unsecure websites is originated from genuine source is something that I would do without being reminded to do so.	1	2	3	4	5
	Checking whether as suspicious, untrusted and	1	2	3	4	5

No	Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
28	unsecure websites or emails are not from fraudulent source is part of my daily routine.					
29	Checking a suspicious, untrusted and unsecure websites or emails before accessing them is something that I feel weird if I do not do it.	1	2	3	4	5
30	I will check the suspicious, untrusted and unsecure websites before accessing any external software programme or email.	1	2	3	4	5
31	I will never open suspicious, untrusted and unsecure websites on my computer.	1	2	3	4	5
32	I will continue to check any suspicious, untrusted and unsecure websites or emails that could attract my attention before accessing them.	1	2	3	4	5
33	I am certain that I would check the suspicious, untrusted and unsecure websites before accessing them.	1	2	3	4	5
34.	I check for the suspicious, untrusted and unsecure websites or emails to ensure that the websites or emails were not from fraudulent sources.	1	2	3	4	5
35.	Sometimes, I don't check for suspicious, untrusted and unsecure websites if doing so affects my performance or productivity.	1	2	3	4	5
36	I only check for the suspicious, untrusted and unsecure websites or emails when it is convenient for me to do so.	1	2	3	4	5
37	When I am busy, I don't check whether the websites or emails I receive were from fraudulent or scammed source.	1	2	3	4	5

Thank you for your assistance

Appendix C: Outliers Assessment Results

Observation number	Mahalanobis d-squared	p1	p2
79	96.6777	.0000	.0000
408	90.4556	.0000	.0000
14	87.2381	.0000	.0000
4	82.6539	.0000	.0000
235	76.8319	0.0002	.0000
18	76.5189	0.0002	.0000
103	76.369	0.0002	.0000
406	73.4652	0.0005	.0000
107	73.3049	0.0005	.0000
182	72.854	0.0006	.0000
410	72.5985	0.0006	.0000
83	72.1609	0.0007	.0000
366	70.6721	0.001	.0000
316	69.5694	0.0013	.0000
145	68.6795	0.0017	.0000
101	66.3563	0.003	.0000
411	65.7315	0.0035	.0000
397	65.6398	0.0035	.0000
407	65.6396	0.0035	.0000
409	64.9849	0.0041	.0000
413	64.4101	0.0047	.0000
169	64.3771	0.0048	.0000
414	63.3834	0.006	.0000
278	63.0221	0.0066	.0000
247	62.7563	0.007	.0000
415	61.3489	0.0096	.0000
349	61.3276	0.0096	.0000
358	59.9939	0.013	.0000
371	59.7655	0.0136	.0000
68	59.4908	0.0144	.0000
335	59.0968	0.0157	.0000
262	59.0661	0.0158	.0000
356	59.0427	0.0159	.0000
156	58.8975	0.0164	.0000
24	58.7323	0.017	.0000
199	58.4629	0.018	.0000
348	58.0544	0.0196	.0000
105	57.8274	0.0206	.0000
1	57.1615	0.0237	.0000
400	57.1306	0.0238	.0000
5	57.0739	0.0241	.0000
80	56.1274	0.0292	.0000
147	55.7326	0.0317	.0000
395	55.1472	0.0356	.0000
268	54.9194	0.0372	.0000
72	54.8172	0.0379	.0000
170	54.5968	0.0396	.0000
90	53.9348	0.045	.0000
304	53.8802	0.0455	.0000
274	53.6822	0.0472	.0000
404	53.5187	0.0487	.0000

164	53.4606	0.0493	.0000
350	53.389	0.0499	.0000
56	53.2757	0.051	.0000
92	52.8873	0.0549	.0000
49	52.8037	0.0557	.0000
382	52.7864	0.0559	.0000
7	52.0992	0.0635	.0000
345	51.5712	0.0698	.0000
336	51.5295	0.0704	.0000
86	51.3772	0.0723	.0000
108	50.9814	0.0776	.0000
332	50.7682	0.0806	.0000
85	50.5883	0.0831	.0000
110	50.0841	0.0907	.0000
261	50.0352	0.0915	.0000
263	49.9185	0.0933	.0000
295	49.9046	0.0936	.0000
181	49.8847	0.0939	.0000
10	49.8001	0.0952	.0000
248	49.7648	0.0958	.0000
188	49.5909	0.0987	.0000
401	49.5882	0.0987	.0000
29	49.1037	0.1071	.0000
16	49.0029	0.1089	.0000
357	48.8883	0.111	.0000
209	48.8793	0.1112	.0000
379	48.8488	0.1117	.0000
405	48.8324	0.112	.0000
54	48.6661	0.1151	.0000
186	48.0991	0.1263	.0000
88	47.988	0.1285	.0000
44	47.6486	0.1357	0.0002
120	47.5187	0.1385	0.0002
159	47.2878	0.1436	0.0004
8	47.1624	0.1464	0.0005
354	47.0164	0.1498	0.0007
183	46.9524	0.1513	0.0006
113	46.7707	0.1556	0.0009
341	46.4939	0.1623	0.0022
223	46.381	0.1651	0.0025
207	46.2453	0.1685	0.0031
402	46.2124	0.1693	0.0024
98	46.1985	0.1697	0.0018
184	46.1558	0.1708	0.0014
25	45.9434	0.1762	0.0026
97	45.8195	0.1795	0.0031
177	45.6181	0.1849	0.0053
254	45.3472	0.1923	0.0114
319	45.2243	0.1958	0.0135

Appendix D: Cook's Distance and Leverage Test Results

No.	COOK'S	LEV	No.	COOK'S	LEV	No.	COOK'S	LEV
1	.00031	.02493	41	.00029	.02244	81	.00056	.01238
2	.00085	.02051	42	.00010	.02391	82	.00236	.03889
3	.00007	.02197	43	.00010	.03372	83	.00003	.03782
4	.00023	.01806	44	.00031	.03203	84	.00042	.03627
5	.00002	.01640	45	.00081	.02950	85	.00000	.01930
6	.00052	.02577	46	.00006	.01749	86	.00227	.01928
7	.00621	.02878	47	.00002	.02886	87	.00550	.02025
8	.00294	.01931	48	.00719	.02287	88	.00118	.01940
9	.00014	.01205	49	.00085	.01180	89	.00239	.02064
10	.00411	.03347	50	.00000	.03525	90	.00076	.01633
11	.00178	.02079	51	.00014	.00996	91	.00039	.00848
12	.00008	.02114	52	.00002	.00272	92	.00011	.01710
13	.00014	.02346	53	.00000	.01722	93	.00237	.00317
14	.00225	.03254	54	.00011	.00989	94	.00061	.01381
15	.00156	.01354	55	.00138	.01931	95	.00579	.02008
16	.00513	.02643	56	.00081	.01251	96	.00003	.01127
17	.00017	.01366	57	.01163	.03196	97	.00002	.00702
18	.02374	.02635	58	.00210	.02789	98	.00013	.02587
19	.00280	.02227	59	.00185	.00651	99	.00004	.01667
20	.00171	.01829	60	.00108	.01770	100	.00114	.00639
21	.00034	.02103	61	.00028	.00351	101	.00284	.02589
22	.00100	.01686	62	.00120	.01557	102	.00000	.00596
23	.00000	.01469	63	.00001	.01098	103	.00164	.02773
24	.01663	.06562	64	.00016	.01519	104	.00038	.02093
25	.00337	.01041	65	.00008	.01324	105	.01395	.01478
26	.00650	.03005	66	.00011	.01526	106	.00175	.03413
27	.00229	.02012	67	.00065	.04019	107	.00103	.03374
28	.00352	.03306	68	.00021	.01738	108	.00415	.01841
29	.00006	.01684	69	.00006	.01063	109	.00276	.00722
30	.00296	.02234	70	.00244	.01311	110	.00003	.00843
31	.00789	.02049	71	.00074	.01432	111	.00037	.02664
32	.00081	.02658	72	.00015	.01072	112	.01480	.03686
33	.01061	.03063	73	.00615	.04364	113	.00889	.02070
34	.00362	.04072	74	.00229	.01955	114	.00311	.03982
35	.00007	.02785	75	.00010	.01149	115	.00091	.02500
36	.00555	.01255	76	.00013	.00666	116	.00541	.00996
37	.00006	.01237	77	.00212	.01749	117	.00002	.02006
38	.00538	.02191	78	.00072	.05119	118	.00196	.02040
39	.00601	.04185	79	.00078	.00966	119	.00281	.01691

40	.00651	.03327	80	.00491	.01886	120	.00006	.03538

No.	COOK'S	LEV	No.	COOK'S	LEV	No.	COOK'S	LEV
121	.00001	.02138	161	.00371	.01667	201	.00045	.01384
122	.00275	.00835	162	.00519	.01781	202	.00023	.01145
123	.00396	.02699	163	.00006	.02280	203	.00003	.00826
124	.00000	.02057	164	.00000	.01066	204	.01536	.01246
125	.00020	.01345	165	.00133	.00763	205	.00009	.01341
126	.00295	.01157	166	.00001	.01860	206	.00330	.02281
127	.00144	.02202	167	.00001	.01350	207	.00084	.01496
128	.00063	.01074	168	.00131	.00915	208	.00380	.01175
129	.00023	.00764	169	.00103	.01605	209	.00020	.00933
130	.00023	.02332	170	.00012	.01627	210	.00268	.00938
131	.00017	.02037	171	.00017	.01365	211	.00015	.01723
132	.00005	.01593	172	.00188	.01307	212	.00000	.01864
133	.00247	.01022	173	.00116	.01330	213	.00704	.02200
134	.00166	.02135	174	.00004	.00655	214	.00410	.01106
135	.00194	.00795	175	.00001	.00225	215	.00340	.01695
136	.00013	.01072	176	.00004	.03001	216	.00315	.01680
137	.00170	.02465	177	.00001	.01309	217	.00292	.02099
138	.00231	.01288	178	.00091	.05316	218	.00138	.01865
139	.00100	.01971	179	.00004	.01317	219	.00018	.02132
140	.00000	.01588	180	.00048	.01193	220	.00030	.01831
141	.00345	.01026	181	.00453	.07446	221	.00642	.01068
142	.00005	.00181	182	.00001	.02577	222	.00012	.01425
143	.00088	.01850	183	.01282	.02988	223	.00151	.01404
144	.00000	.01595	184	.00016	.02502	224	.00390	.01501
145	.00001	.02911	185	.00001	.00958	225	.00111	.00804
146	.00014	.01737	186	.00004	.02201	226	.00165	.00596
147	.00132	.01497	187	.00007	.02879	227	.00219	.00687
148	.00216	.00628	188	.00036	.03105	228	.00038	.01958
149	.00565	.01530	189	.00004	.01167	229	.00022	.01360
150	.00299	.00796	190	.00005	.00999	230	.00005	.00488
151	.00591	.03086	191	.00000	.00477	231	.00002	.00663
152	.00075	.00977	192	.00002	.02181	232	.00184	.02382
153	.00019	.01620	193	.00002	.01192	233	.00262	.01254
154	.00107	.01699	194	.00010	.01620	234	.00032	.01509
155	.00013	.00915	195	.00450	.01592	235	.00006	.00889
156	.00000	.02361	196	.00397	.00963	236	.00005	.01397
157	.00094	.04663	197	.00036	.01905	237	.00004	.00588
158	.00094	.00822	198	.00030	.01993	238	.00030	.01027
159	.00188	.02410	199	.00369	.02101	239	.00058	.01489
160	.00001	.02138	200	.01123	.02251	240	.00270	.01026

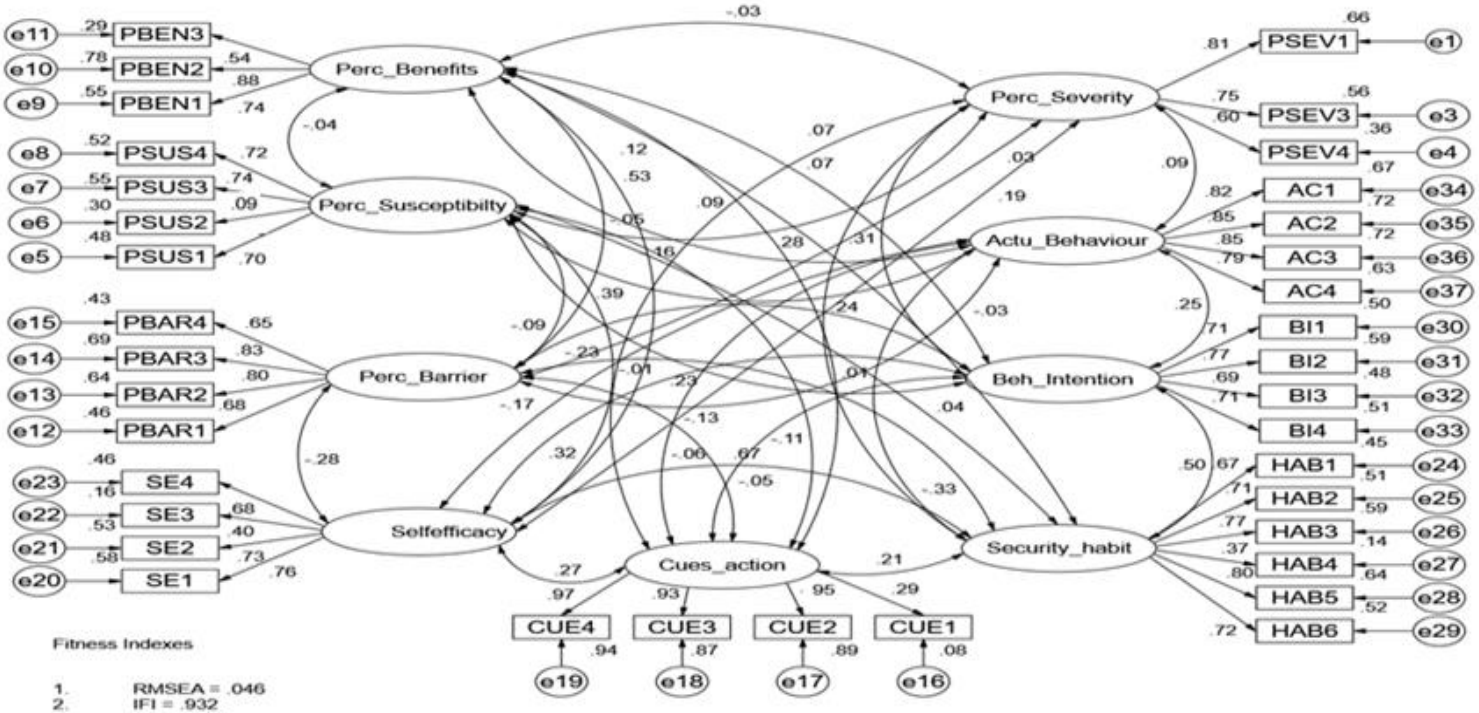
No.	COOK'S	LEV	No.	COOK'S	LEV	No.	COOK'S	LEV
241	.00431	.01660	281	.00003	.01839	321	.00338	.02534
242	.00283	.00788	282	.00021	.02623	322	.00778	.02617
243	.00014	.01127	283	.00012	.00642	323	.00384	.01273
244	.00227	.03049	284	.00014	.00993	324	.00009	.01974
245	.00357	.02975	285	.00011	.01033	325	.00044	.01390
246	.00245	.00659	286	.00008	.01630	326	.00003	.01499
247	.00305	.00851	287	.00125	.01874	327	.00005	.01332
248	.00502	.02142	288	.00389	.02282	328	.00003	.01908
249	.00009	.01261	289	.00440	.01714	329	.00966	.02471
250	.00674	.01640	290	.00049	.01190	330	.00000	.02040
251	.00560	.01440	291	.00002	.00832	331	.00070	.02184
252	.02230	.02203	292	.00000	.01245	332	.00005	.00896
253	.00626	.01082	293	.00119	.02610	333	.00219	.05196
254	.00510	.00839	294	.00463	.02313	334	.00094	.02288
255	.00012	.00551	295	.01135	.02212	335	.00231	.03362
256	.00010	.00818	296	.00000	.01179	336	.00533	.02365
257	.00016	.00824	297	.00027	.01857	337	.00365	.02431
258	.00000	.01186	298	.00007	.01182	338	.00651	.02985
259	.00092	.00896	299	.00010	.00525	339	.00008	.02548
260	.00025	.00905	300	.01820	.01295	340	.00732	.03913
261	.00947	.02020	301	.00015	.01103	341	.00259	.04749
262	.00286	.00967	302	.00264	.02018	342	.00654	.01956
263	.00027	.01377	303	.00072	.00928	343	.00410	.01196
264	.00093	.01335	304	.00336	.01396	344	.00291	.03213
265	.00464	.01291	305	.00328	.03196	345	.00053	.02674
266	.00023	.02794	306	.00349	.00963	346	.00636	.02964
267	.00003	.02414	307	.00012	.00815	347	.00695	.03840
268	.00004	.02437	308	.00023	.01160	348	.02558	.01472
269	.00032	.02390	309	.00200	.00562	349	.00397	.01133
270	.00054	.03031	310	.00285	.01312	350	.01019	.01860
271	.00594	.01411	311	.00373	.01419	351	.00032	.01381
272	.00021	.00900	312	.00272	.01945	352	.00053	.01616
273	.00035	.01079	313	.00520	.02788	353	.01177	.02023
274	.00010	.00993	314	.00052	.02603	354	.00443	.02527
275	.00623	.01606	315	.00006	.00742	355	.00002	.01453
276	.00948	.03778	316	.00004	.01595	356	.06365	.09317
277	.00006	.03459	317	.00934	.01814	357	.00534	.02264
278	.02072	.01424	318	.00039	.02110	358	.00003	.01144
279	.00015	.01373	319	.00075	.01375	359	.00000	.01325
280	.00061	.01871	320	.00236	.00873	360	.01680	.04625

No.	COOK'S	LEV	No.	COOK'S	LEV
361	.01049	.04881	401	.00002	.01225
362	.00029	.02017	402	.00002	.02789
363	.00043	.01403	403	.00001	.01666
364	.00193	.07294	404	.00617	.02542
365	.00018	.02367	405	.00578	.02180
366	.00001	.03047	406	.00470	.02165
367	.00074	.01775	407	.00878	.03514
368	.00033	.00549	408	.00506	.01578
369	.00098	.00944	409	.00054	.01600
370	.00060	.01692	410	.00006	.01237
371	.01057	.02176	411	.01147	.03431
372	.00002	.02129	412	.00003	.02762
373	.00005	.01744	413	.01914	.03483
374	.00015	.01727	414	.00003	.01216
375	.00100	.02718	415	.00002	.02124
376	.00009	.01961			
377	.00003	.03199			
378	.00026	.01818			
379	.00016	.01183			
380	.00001	.02376			
381	.00002	.00715			
382	.00031	.02313			
383	.00353	.02320			
384	.00355	.01735			
385	.00057	.01470			
386	.00000	.01457			
387	.00006	.03356			
388	.00070	.03331			
389	.00474	.01914			
390	.00888	.01956			
391	.00010	.01250			
392	.00000	.01703			
393	.00007	.01257			
394	.00093	.03139			
395	.00000	.01671			
396	.00177	.02859			
397	.00003	.01623			
398	.00274	.02032			
399	.00757	.02677			
400	.00881	.02647			

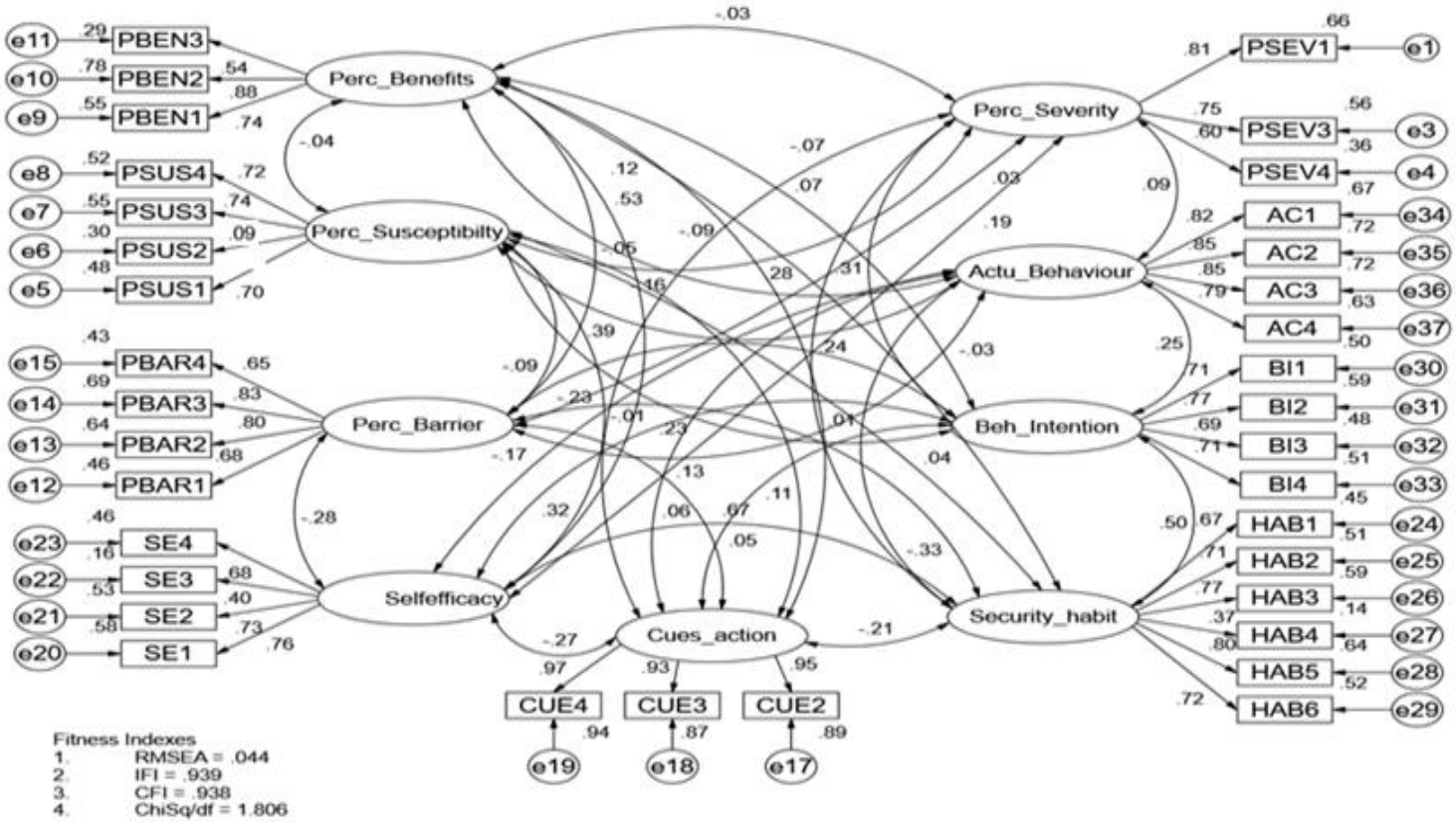
Appendix E: Correlations Estimates for Constructs

Construct/ Variable	Paths	Construct/ Variable	Estimates
Perc_Severity	<-->	Perc_Benefits	-.030
Perc_Severity	<-->	Security_habit	.236
Perc_Severity	<-->	Perc_Susceptibilty	.263
Perc_Benefits	<-->	Perc_Barrier	-.055
Perc_Benefits	<-->	Selfefficacy	.524
Perc_Benefits	<-->	Actu_Behaviour	-.162
Perc_Barrier	<-->	Beh_Intention	-.228
Perc_Barrier	<-->	Security_habit	-.322
Selfefficacy	<-->	Security_habit	.666
Cues_action	<-->	Actu_Behaviour	.056
Perc_Susceptibilty	<-->	Cues_action	.131
Security_habit	<-->	Actu_Behaviour	.004
Perc_Susceptibilty	<-->	Actu_Behaviour	.369
Perc_Susceptibilty	<-->	Security_habit	.037
Perc_Susceptibilty	<-->	Perc_Barrier	-.081
Perc_Benefits	<-->	Security_habit	.106
Perc_Severity	<-->	Perc_Barrier	.032
Perc_Severity	<-->	Actu_Behaviour	.094
Security_habit	<-->	Beh_Intention	.504
Beh_Intention	<-->	Actu_Behaviour	.249
Perc_Severity	<-->	Beh_Intention	.311
Perc_Barrier	<-->	Actu_Behaviour	-.027
Cues_action	<-->	Beh_Intention	.047
Perc_Benefits	<-->	Cues_action	-.088
Perc_Barrier	<-->	Cues_action	.126
Perc_Severity	<-->	Cues_action	-.069
Perc_Susceptibilty	<-->	Perc_Benefits	-.035
Perc_Benefits	<-->	Beh_Intention	.074
Cues_action	<-->	Selfefficacy	-.279
Cues_action	<-->	Security_habit	-.210
Selfefficacy	<-->	Beh_Intention	.318
Selfefficacy	<-->	Actu_Behaviour	-.189
Perc_Susceptibilty	<-->	Beh_Intention	.217
Perc_Barrier	<-->	Selfefficacy	-.285
Perc_Susceptibilty	<-->	Selfefficacy	-.033
Perc_Severity	<-->	Selfefficacy	.173

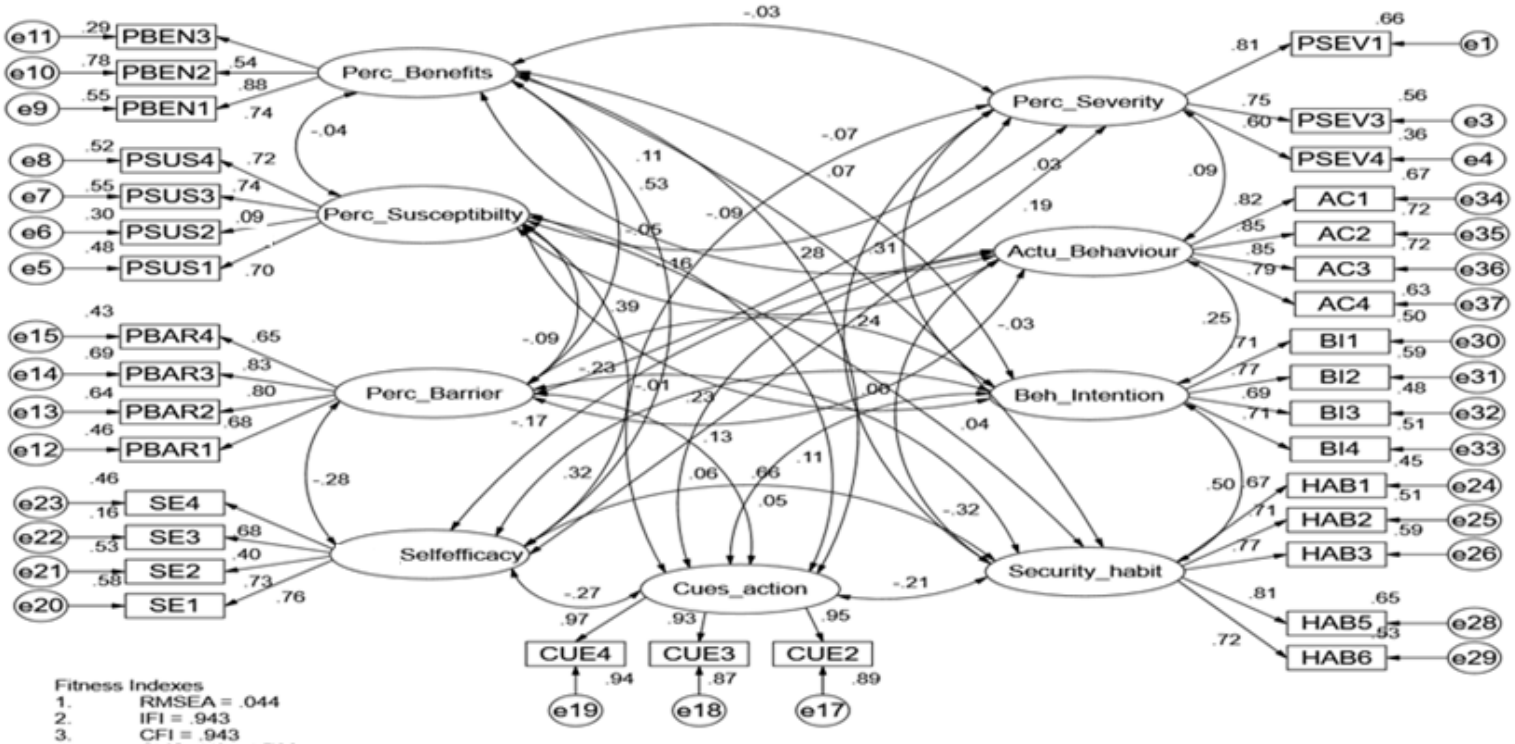
Appendix F: Adjusted Measurement Model: Item PSEV 2 Deleted



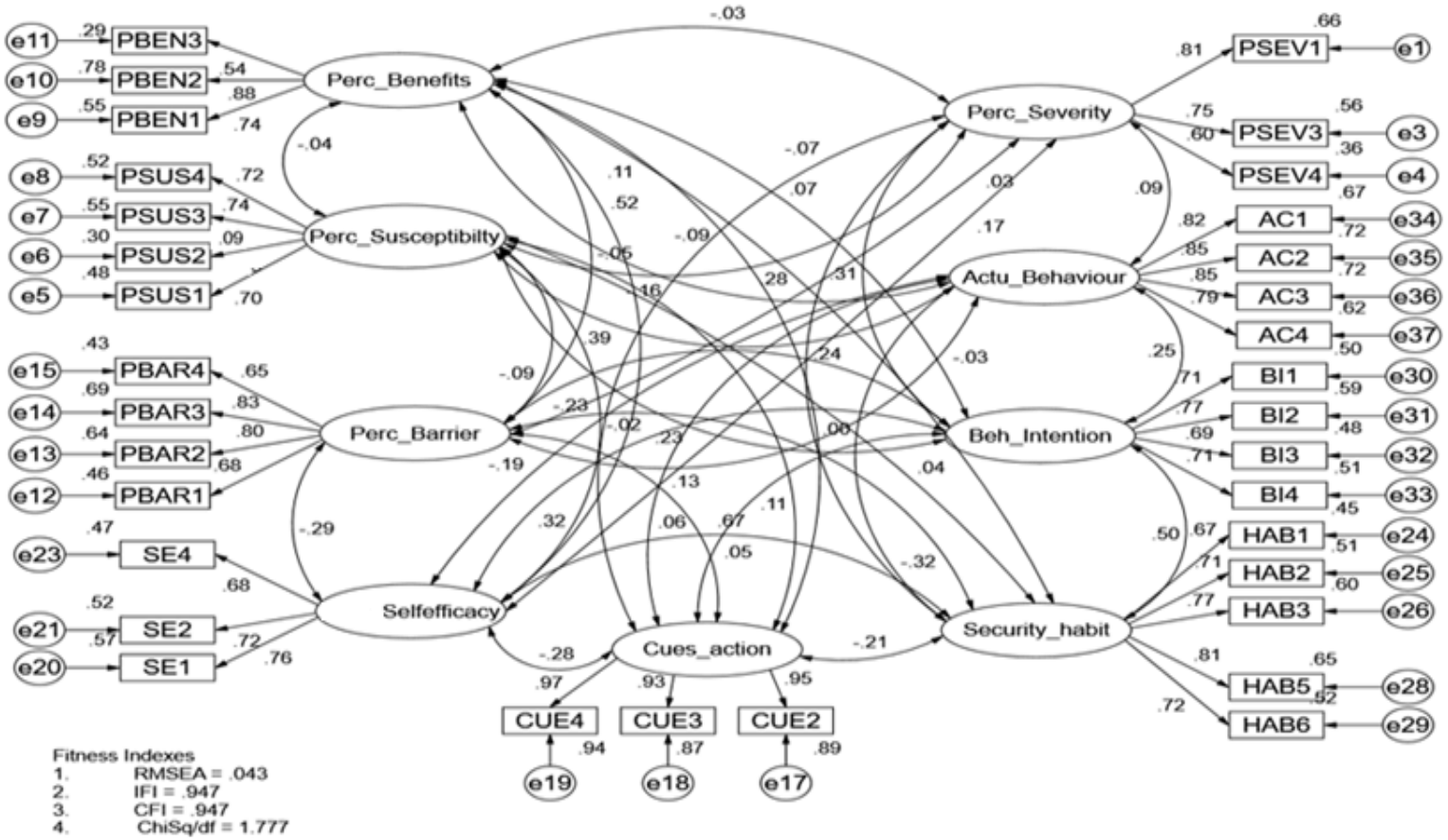
Appendix G: Adjusted Measurement Model: Item CUE 1 Deleted



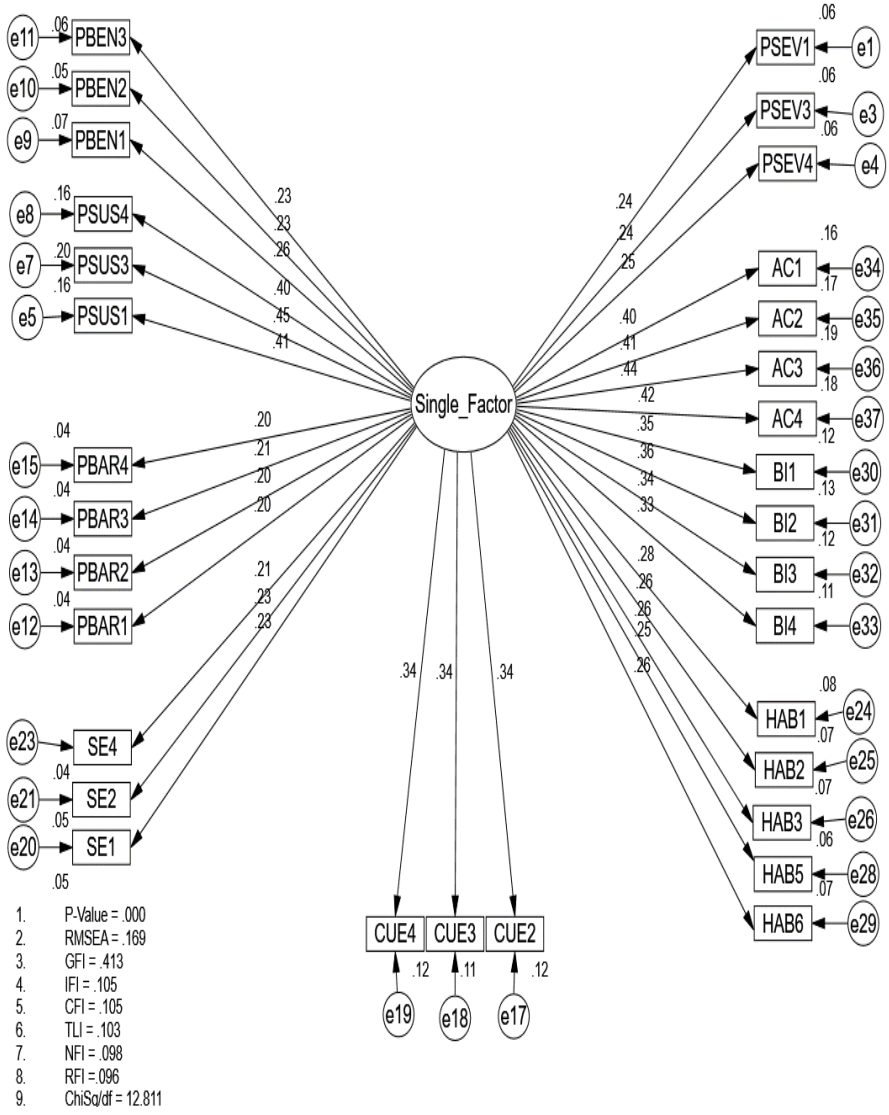
Appendix H: Adjusted Measurement Model: Item HAB4 Deleted



Appendix I: Adjusted Measurement Model: Item SE3 Deleted



Appendix J: CMV Results –Harman's Single Factor Test



Appendix K: Constructs Studied in the Past Studies

Constructs	Role	Model/ Theory
Perceived sanctions severity [a,b, c, d]	Independent variable	
Perceived detection certainty [a ,b, c, d]	Independent variable	GDT
Perceived sanction [a, b, c, d]	Independent variable	
Behaviour intention [a, b ,c, d]	Dependent variable	
Perceived severity [e,f,g,h,I,j,k,l,m]	Independent variable	
Perceived susceptibility [e,f,g,h,I,j,k,l,m]	Independent variable	
Perceived benefits [e,f]	Independent variable	HBM
Perceived barriers [e,f]	Independent variable	
Self-efficacy [e,f,g,h,I,j,k,l,m]	Independent variable	
Cues to action [e.f]	Independent variable	
Age, gender, prior experience [e]	Moderating variable	
Behaviour [e.f]	Dependent variable	
Perceived severity [e,f,g,h,I,j,k,l,m]	Independent variable	
Perceived susceptibility [e,f,g,h,I,j,k,l,]	Independent variable	
Fear arousal [m]	Independent variable	PMT
Response-efficacy/ Self-efficacy [e,f,g,h,I,j,k,l,m]	Independent variable	
Response costs [g,I,j,k,l]	Independent variable	
Motivation / Behaviour intention [a ,b, c, d ,n,m]	Dependent variable	
Attitude [n,o]	Independent variable	TPB/TRA
Social Norms [n,o]	Independent variable	
Perceived Behavioural Control [n,o]	Independent variable	
Behavioural intention [a, b, c, d ,n,o]	Dependent variable	
Perceived severity [e,f,g,h,I,j,k,l,m]	Independent variable	
Perceived susceptibility [e,f,g,h,I,j,k,l,m]	Independent variable	
Perceived Threats [m]	Independent variable	
Safeguards effectiveness [m]	Independent variable	TTAT
Safeguards costs [m]	Independent variable	
Self –efficacy [e,f,g,h,I,j,k,l,m]	Independent variable	
Avoidance motivation [m]	Independent variable	
Avoidance behaviour [m]	Dependent variable	
General security orientation [f]	Independent variable	Additional

Security awareness [p]	Independent variable	factors
Habit [q]	Independent variable	
Prior experience [p]		

Sources:

[a] D'Arcy and Hovav (2004)
[b] Gibbs (1968)
[c] Weaver and Carroll (1985)
[d] Herath and Rao (2009)
[e] Claar and Johnson (2012)
[f] Ng et al. (2009)
[g] Herath and Rao (2009)
[h] Davinson and Sillence (2010)
[I] Siponen et al. (2006)
[j] Vance, Siponen and Pahnilla (2012)
[k] Crossler and Belanger (2014)
[l] Johnson and Warkentin (2010)
[m] Liang and Xue (2009, 2010)
[n] Ifinedo (2012)
[o] Ng and Rahim (2005)
[p] Mahabi (2010)
[q] Yoon et al. (2012) and Yoon (2011)

BIODATA OF THE STUDENT

Daniel Ntabagi Koloseni, Lecturer in Information Systems, Faculty of Computing, Information Systems and Mathematics
The Institute of Finance Management, Tanzania

He obtained his Advanced Diploma in Information Technology (IFM, Tanzania) and Master Degree in Information Security and Biometrics (Kent, UK) in 2006 and 2008 respectively. He is the lecturer in information systems and related subjects and currently pursuing PhD at University Tunku Abdul Rahman (UTAR), Malaysia.

His teaching experience includes, teaching Enterprise Resource Planning Systems, Business Processes and Information Technology, Business Information Systems, Information Technology in Organizations, Information security and Audit control, Management of Technology and Innovation and Biometrics Technology and Standards.

He has been active researcher since 2011. From 2011 to date he has organized and conducted several workshops, seminars, training and consultancies in ICT. Daniel has authored several journal articles, conference papers and three book chapters.

Daniel's research interest lies in Enterprise Resource Planning systems design and implementation, E-learning systems, Social media, Information Security behaviours, ICT policies and Security education, training and awareness

programme (SETA). Others are business processes and Strategy formulation, biometrics authentication technologies and E- wastes management.

During his PhD studies, he has published one conference paper and submitted two journal articles as follows:

Koloseni, D., Chong, Y.L & Gan, M.L (2015). The Practice of Information Security Behaviour among Government's Employees in Tanzania: A Conceptual Framework Using Health Belief Model (HBM). *International Conference on Business, Accounting, Finance, and Economics, BAFE 2015*

The two journal articles submitted:

Accepted Article

Koloseni, D., Chong, Y.L & Gan, M.L (2017).Understanding Information Security Behaviours of Tanzanian Government Employees: A Health Belief Model Perspective. *International Journal of Technology and Human Interactions, 15(1)*

Under review Article

Koloseni, D., Chong, Y.L & Gan, M.L (xx). Security Policy Compliance in Public Institutions: An Integrative Approach of Health Belief Model, Employee's Commitment and Information Security Awareness. *Journal of Applied Structural Equation Modeling (JASEM)*

From the year 2011 to date, he has published the following articles. The list does not include publications related to PhD research.

Journals

Koloseni, D (2015). Security, Privacy Awareness vs. Utilization of Social Networks and Mobile Apps for Learning: Student's Preparedness. *Advances in Computer Science: An International Journal,* 4(3), 111-117.

Koloseni, D., & Sengati, F. (2016). An Assessment of the Adoption and Usage of ICT in Tanzania Public Sector. *The African Journal of Finance and Management*, 22 (2)

Koloseni, D., & Mandari, H (2017). The Role of Personal Traits and Learner's Perceptions on the Adoption of E-Learning Systems in Higher Learning Institutions. *The African Journal of Finance and Management* 26 (1), 61-75.

Mandari, H., & Koloseni, D. (2016). Biometrics Authentication in Financial Institutions: The Intention of Banks to Adopt Biometric Powered ATM. *Advances in Computer Science: An International Journal, 5(4), 9-17.*

Mandari, H., & Koloseni, D. (2017). Electronic Fiscal Device (EFD) Acceptance for Tax Compliance Among Trading Business Community in Tanzania: The Role of Awareness and Trust. *International Journal of Economics, Commerce and Management*, *5*(3), 142–158.

Michael, R., Shimba, F., & Koloseni, D. (2012). The Impact of Configurations on the Performance of Server Based Computing. *Journal of Information Technology Review Volume*, *3*(2), 95–103.

Njoroge, C.N., & Koloseni, D. (2015). Adoption of Social Media as Full-Fledged Banking Channel : An Analysis of Retail Banking Customers in Kenya. *International Journal of Information and Communication Technology Research*, *5*(9).

Book Chapters

Koloseni, D. (2015). Perception of Tanzanian Small and Medium Enterprises(SMES)on Adoption of ICT. In *Socio- economic Development in Tanzania : A Multidisciplinary Perspective (pp. 184–194). Dar es Salaam, Tanzania: University Press.*

Koloseni, D., Otaigo, E., & Msangawale, A (2012). Towards Utilization of National ICT communication backbone : Key Issues. In *Frontiers of Information Technology*.*(pp.1–9).Masaum Publishers*

Koloseni, D., & Shimba, F.(2012). E-Waste Disposal Challenges and Remedies : A Tanzanian Perspective. In *Waste Management - An Integrated Vision(pp. 333–348).InTech*.

Conference Papers

Koloseni, D., Msangawale, A., & Otaigo, E. (2011). Issues towards Utilization of Fiber Optic Communication : The Case of Seacom Submarine Fiber Optic Cable in Tanzania Issues towards Utilization of Fiber Optic Communication : The Case of Seacom Submarine Fiber Optic Cable in Tanzania. *In ICT 211 The 5th International Conference on Information Technology. Amman, Jordan: Al-Zaytoonal University.*

Koloseni, D., & Omary, Z. (2011). Towards Using Social Networks and Internet-Enabled Mobile Devices for Learning: Students' Preparedness. *In International Conference on Informatics Engineering and Information Science (pp. 13–21). Springer.*

Machupa, O., Otaigo, E., Koloseni, D., & Shimba, F. (2011). Assessing the factors influencing information technology investment decisions: A survey of sampled public sector organizations in Tanzania. In *Communications in Computer and Information Science (Vol. 251 CCIS, pp. 385–399). Springer*.

Pazi, S., Koloseni, D., & Shimba, F. J. (2013). Last mile connectivity issues facing Tanzania National ICT backbone. In *The International Conference on E-Technologies and Business on the Web (EBW2013); Conference proceeding*

Shimba, F., Koloseni, D., & Michael, R. (2012). Technology assisted teaching and learning methods: The Institute of Finance Management. 2012 *International Conference on Education and E-Learning Innovations, ICEELI 2012.*