

**THE ELEMENTS FOR DEVELOPING INFORMATION TECHNOLOGY  
SECURITY METRICS MODEL FOR UNIVERSITIES IN KENYA**

**CHARLES OCHIENG' OGUK**

**A Thesis Report Submitted to the Institute of Postgraduate Studies, in Partial  
Fulfilment of the Requirements for the Award of the Doctor of Philosophy Degree in  
Information Technology (Security and Audit).**

**KABARAK UNIVERSITY**

**JULY, 2018**

## DECLARATION

This research thesis is my own work and to the best of my knowledge it has not been presented for the award of a degree in any other university.

Signed .....Date:.....

**Charles Ochieng' Oguk**

**GDI/M/1353/09/15**

## RECOMMENDATION

To the Institute of Postgraduate Studies:

The research thesis entitled “**Investigating Elements for Developing Information Technology Security Metrics' Model for Universities in Kenya**” and written by **Charles Ochieng' Ogiuk** is presented to the Institute of Postgraduate Studies of Kabarak University. We have reviewed the research thesis and recommend it to be accepted in partial fulfilment of the requirement for the Degree of Doctor of Philosophy in Information Technology (Security and Audit).

Sign:



Date: July 27, 2018

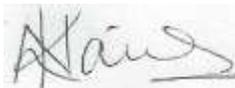
**PROF. KEFA RABAH, PhD.**

Professor of Physics & ICT

School Of Computer Science and Bio-Informatics

Kabarak University

Sign:



Date: July 27, 2018

**DR. NICKSON M. KARIE, PhD**

Senior Lecturer

School Of Computer Science and Bio-Informatics, Kabarak University

## **ACKNOWLEDGMENT**

I wish to recognize the guidance from my supervisors Prof. Kefa Rabah, and Dr. Nickson Karie, for their valued pieces of advice which made this research work a success. Their contributions made the research work to be completed within the appropriate time. I honestly appreciate their fruitful critiques and close follow-ups in making this research work a reality. Further, I recognize the assistance of Mr. Roy Obiero for his dedication in developing codes for the metric's program codes. In addition, I acknowledge the contributions of Prof. Karume for conceiving the IT security metrics' idea, Dr. Thiga for his advice on metrics' dashboard, Dr. Omollo for general advice on thesis writing, Dr. Oyiengo for reviews, Mr. Rakama, Dr. Maghanga for statistical help and Dr. Okello for research methodology advice. Most importantly, I give all thanks to God for his divine cover and counsel in finalizing this research work.

## **COPYRIGHT**

© 2018

Charles Ochieng' Oduk

All rights reserved. No part of this Thesis may be reproduced or transmitted in any form by means of either mechanical, including photocopying, recording or any other information storage or retrieval system without permission in writing form the author or Kabarak University.

## ABSTRACT

There has been increased frequency of information systems' security breaches within universities. Studies indicate that information technology security management could be improved if IT security management were used together with appropriate security metrics which are based on major elements of information technology security. However, there is continued application of inappropriate metrics within the universities. As such, estimating information security status remains a challenge, making managing IT security difficult. The objectives of this study were: to investigate the major elements in management of information security within universities in Kenya, to investigate the relationship between the implementation of the major elements and metrics in the universities in Kenya, to develop and test applicability of a suitable information technology security implementation metrics model based on major information technology security elements for universities in Kenya. Three-step methodological approach was adopted as based on goal-question-metrics concepts and theory of measurement. Step one was a review of secondary publications to ascertain the major information technology security elements and seek the extent of application of the elements within the universities. Secondly, 91 respondents from the 70 universities in Kenya were sampled for data collection. Purposive sampling was conducted for data collection using questionnaire and an interview schedule. In each sampled university, 13 operation areas related to information systems were considered, giving a total of 91 respondents. Data was collected from the team leader of each operation area, then analysed using SPSS, where the mean and regression model was adopted. Results showed that while security management is conducted with respect to IT security elements, their levels of implementation remain inadequate. Significant relationship and dependence was found between IT security elements and metrics. Regression coefficient of IT security elements were found and used to develop a reliable IT security metrics' prototype aided by measurement scales and color codes corresponding to different security situations. Applicability of the model was tested at (<http://41.89.203.228/oguk>) and found feasible. In conclusion, there is statistically significant relationship between the metrics and implementation of the elements; wherein, while the level of implementation of IT security elements was found to contribute to the metrics, information security policy was found to contribute more. Therefore, it is recommended that the developed IT security implementation metrics model be used together with the security policy for better information systems security management. The model is recommended for policy makers.

**Keywords:** IT security metrics, IT security elements, metrics models, metrics dashboard, metrics program, goal question metrics, security measurement scaling.

## TABLE OF CONTENTS

DECLARATION .....	ii
RECOMMENDATION .....	iii
ACKNOWLEDGMENT.....	iv
COPYRIGHT .....	v
ABSTRACT.....	vi
TABLE OF CONTENTS.....	vii
THE LIST OF SYMBOLS AND ABBREVIATIONS .....	xiii
OPERATIONAL DEFINITION OF TERMS .....	xiv
CHAPTER ONE .....	1
INTRODUCTION .....	1
1.1 Introduction.....	1
1.2 Background to the Study.....	1
1.2.1 The Dependency of Universities on Information Technology.....	2
1.2.2 Information Technology Security Challenges in Universities .....	4
1.2.3 Metrics Factor in Information Technology Security Management .....	6
1.2.4 IT Security Metrics .....	6
1.2.5 The Elements' Factors in Information Technology Security Management.....	7
1.3 Statement of the Problem.....	10
1.4 Purpose of the Study .....	12
1.5 Objectives of the Study .....	12
1.6 Research Questions.....	12
1.7 Justification / Significance of the Study .....	12
1.8 Scope of the Study .....	13
1.9 Limitations of the Study.....	13
1.10 Assumption of the Study.....	14
CHAPTER TWO .....	15
LITERATURE REVIEW .....	15
2.1 Introduction.....	15
2.2 General Overview of Literature Related to the Main Concepts .....	15
2.2.1 Role of Standards in IT Security Metrics and Management .....	15
2.2.2 International Organization for Standardization (ISO) 27001 .....	18
2.2.3 Control Objectives for Information and Related Technology (COBIT) .....	19
2.2.4 Goal - Question - Metrics (GQM) Concept .....	21
2.2.5 The GQM Step in Metrics' Modeling Process.....	22
2.2.6 Color Codes Concept for General Security Metrics.....	23
2.2.7 Color Codes in IT Security Management.....	24
2.2.8 Metrics Presentation in Color-Codes .....	25
2.2.9 IT Security Metric's Dashboard .....	25

2.3	The Elements in IT Security Management in Universities .....	27
2.3.0	The Major Elements of IT Security Management.....	29
2.3.1	IT Security Policy .....	29
2.3.2	Physical Security.....	31
2.3.3	Network Security .....	33
2.3.4	Data Security.....	36
2.3.5	Access Control .....	40
2.4	The Relationship Between the Major IT Security Elements' Metrics.....	44
2.4.2	Information Technology Security Metrics.....	46
2.4.3	Source of Data for IT Security Metrics.....	48
2.4.4	Categories of IT Security Metrics.....	49
2.4.5	SMART Metrics : Communication of Metrics to Executives.....	51
2.4.8	The Gap to be Addressed by Objective two.....	56
2.5	The Existing IT Security Metric's Model .....	56
2.5.1	OCTAVE .....	57
2.5.2	Common Vulnerability Scoring System (CVSS).....	57
2.5.4	Gaps in the Models: .....	63
2.6	THEORETICAL FRAMEWORK .....	64
2.6.1	The Theory of Measurement.....	64
2.6.2	Measurement Approach .....	65
2.6.3	Importance of Measurement Theory.....	65
2.6.4	Limitations to Measurement Theory.....	66
2.6.5	Theories Applied in Adoption and Implementation of ICT Systems.....	66
2.6.6	A Review of the Theory of Reasoned Action .....	66
2.6.7	Theory of Planned Behavior (TPB) .....	67
2.7	Conceptual Framework.....	69
2.7.1	Conceptual Framework Explained.....	70
CHAPTER THREE .....		72
METHODOLOGY .....		72
3.1	Introduction.....	72
3.2	Research Design.....	72
3.2.1	Steps in Research Design.....	72
3.2.2	Identifying Information Technology Security Elements in Universities in Kenya.....	73
3.3	Location of the Study.....	74

3.4	Target Population.....	74
3.5	Sampling Procedure and Sample Size .....	74
3.5.1	Sampling Procedure.....	74
3.6	Research Instruments .....	78
3.6.2	The Validity of the Instrument.....	79
3.6.3	Reliability of the Instrument .....	79
3.7	Data Collection Procedure .....	80
3.8	Data Analysis .....	80
3.8.1	Use of the Average gap Scales for IT Security Metrics.....	81
3.8.2	Regression Analysis for IT Security Metrics' Model.....	82
3.8.3	The IT Metrics' Model.....	82
3.8.4	GQM Steps for the IT Security Metrics Model.....	83
3.8.5	The IT Security Metrics' Model implementation and Testing .....	84
3.8.6	Prototype Development.....	84
3.8.7	Program Code for IT Security Model .....	85
3.9	The Ethical Considerations .....	85
<b>CHAPTER FOUR.....</b>		<b>86</b>
<b>DATA ANALYSIS, PRESENTATION AND DISCUSSION.....</b>		<b>86</b>
4.1	Introduction.....	86
4.2	General and Demographic Information .....	86
4.3	The Findings Addressing Objective one.....	90
4.3.1	Identifying Information Technology Security Elements.....	90
4.3.3	Element One: Information Technology Security Policy (SP).....	90
4.3.4	Element Two: Physical Security for Information Systems .....	93
4.3.5	Element Three: Network Security.....	94
4.3.6	Element Four: Data Security.....	97
4.3.7	Element Five: System Access Control.....	99
4.4	Findings Addressing objective two and Objective Three .....	101
4.5.0	Regression Analysis for IT Security Metrics' Model.....	101
4.5.1	Contribution by IT Security Policy in the Model.....	104
4.5.2	Physical Security.....	105
4.5.3	Network Security .....	106

4.5.4	Data Security.....	107
4.5.5	Access Control.....	107
4.6	The Unique Ratio Coefficient.....	108
4.6.1	Scaling of the IT Security Metrics.....	109
4.6.2	Measurement Approach.....	109
4.6.3:	Deriving the Values for the Minimum and the Maximamun Values.....	110
4.6.4	Metrics' Presentation in Color-Code.....	111
4.7	Evaluation the Applicability of the IT Security Metrics' Model.....	112
4.7.0	Evaluating the IT Security Metric's Model.....	112
4.7.1	GQM Steps for the Model.....	112
4.7.3	The IT Security Metrics' Model Implementation.....	112
4.7.4	Applicability of the IT Security Metrics' Model.....	113
CHAPTER FIVE.....		120
CONCLUSION AND RECOMMENDATIONS.....		120
5.0	Introduction.....	120
5.1	Limitations and De-Limitations.....	120
5.2	Implications for Practice.....	120
5.3	CONCLUSIONS.....	121
5.4	RECOMMENDATIONS.....	122
REFERENCES.....		125
APPENDICES.....		143
Appendix 1 : Questionnaire type 1: for Information Systems Users Only.....		143
Appendix 2 :Questionnaire type 2: for ICT Personnel Only.....		146
Appendix 3: Interview schedule.....		149

## THE LIST OF TABLES

Table 4.15: Starting Point .....	113
Table 4.13:Regression Analysis.....	102
Table 4.16 : IT Security Policy Measurement .....	114
Table 4.17: Physical Security Measurement.....	115
Table 4.18: Network Security Measurement .....	116
Table 4.19: Access Control Measurement .....	117
Table 4.20: Data Security Measurement.....	118
Table 4.14: Metrics' Presentation in Color-Code.....	111
Table 4.6 : Access Control Mechanism Applied .....	100
Table 4.7: Nature of Authentication to Access Server Room.....	100
Table 4.4: Total Internet Bandwidth Levels in the University .....	94
Table 4.5: Availability of Network Security Features .....	96
Table 4.3: Level of Adoption of IT Security Policy Elements within the Universities.....	91
Table 4.1: Gender of the Respondents .....	87
Table 4.2: Institution of the Respondents .....	87
Table 4.3: Age group of the Respondents.....	87
Table 4.4: Education Levels of the Respondents .....	88
Table 4.2: Area of the University .....	88
Table 3.1: The University Population and the Sample .....	76
Table 3.2: Purposive Sample sampling .....	78
Table 2.1: Conceptualized Metrics' Presentation in Color-Code.....	25

## LIST OF FIGURES

Figure 2.1: Johnson's PDCA Quality Progress chat .....	18
Figure 2.2: Cobit 5 Enablers: .....	19
Figure 2.3: The Conceptual Framework .....	69

## THE LIST OF SYMBOLS AND ABBREVIATIONS

### List of Symbols

$\chi^2$	Chi-square
$Q_M$	IT security metrics
$p$	Probability value
$\beta$	Beta value of the coefficient of in-dependent variable

### List of Abbreviations and Acronyms

AC	Access Control
APT:	Advanced Persistent Threat.
BYOD	Bring Your Own Device
CAK:	The Communications Authority Of Kenya
CANN	Cluster Centre And Nearest Neighbour
DS	Data Security
IDS	Intruder Detection System
ICT:	Information and Communication Technology
IT	Information Technology
ITIL	IT Infrastructure Library
KPI	Key Performance Indicator
NDUS	North Dakota University System
NS	Network Security
PS	Physical Security
ROI	Returns on Investment
ROSI	Return On Security Investment
SP	Security Policy
SCADA	Supervisory Command Data Acquisition
SMART	Specific, Measurable, Achievable, Realistic and Time-bound
SMEs	Small and Medium Enterprises
VLANs	Virtual Private Networks

## OPERATIONAL DEFINITION OF TERMS

Asset	Information assets are composed of computer networks, any system, device, and personnel that collectively have computing value to a given organization. Information asset includes computer hardware, system applications, and the data therein.
Authorization	Process of granting rights of accessing information resources. This is done through resources like active directories.
Authentication	Process of confirming whether system users, according to a given databases, are actually who they claim to be while trying to access a system's resources. It is normally accomplished by checking user bio-metrics access control, names and passwords, retina scanning and smart cards.
Automation systems	Computer systems that are used to reduce or replace manual operations in organizations.
Communications Authority of Kenya	It is a communication regulation corporation that is mandated to steer telecommunications functions, including broadcasting and general information technology regulation in Kenya.
Cyber	Any inter-connection of computer systems with internet connectivity
Cyber-criminals	Perpetrators of computer crimes who exploit internet as the main link to the computer systems they compromise.
Elements of IT Security	The major operational building blocks of robust and secure information systems that holistically constitute the parameters along which managing IT security is executed.
Information and Communication Technology	Stands for "information and communication technology", ICT usually encompasses the combination of long distance signal transfer and manipulation at the terminal destinations. Usually, it combines telecommunication and information technology as it involves all equipment, system applications and services that facilitate communication for Computers, televisions, cell phones, radios and satellite systems. Arguably, ICT also involves people, especially the users and the administrators of systems. Preservation of confidentiality, integrity and availability of information.
IT Security Metrics	This is a special measurement generated from analysis and interpretation of data collected on elements of information technology, as the data is believed to give direction on the levels of implementation and management of the elements of information technology security in a given institution.
Information Security Metrics Model	A low level system of measurement that relies on analysis of data collected on the performance levels associated with elements of information technology, to give

status of IT security in an organization.

Plan-Do-Check-Act	Is a four-stage repetitive model for continuous improvement in IT security management process
Risk	A combination of the likelihood of threat occurrence, the likelihood of resultant undesirable effects, and the extent of severity of the resulting undesirable effect.
Sneaker net	Physically transferring of electronic information from one computer system to another by using portable external storage devices like memory cards, flash-disks, CD or other removable medium.
Threats:	Circumstances that could possibly compromise the data confidentiality, Integrity and availability.

## **CHAPTER ONE**

### **INTRODUCTION**

#### **1.1 Introduction**

This section contains: a brief review of background to the study which considers the increasing attacks on university information systems, IT security management and measurement approaches applied in the university. It has a sub-section on the dependency of universities on Information Technology (IT); where the use of information systems in automating academic and administrative functions is discussed. It then reviews the consequent information technology security challenges in universities, the metrics and the IT security elements' factors in information technology security management, statement of the problem, objectives, specific objectives, research questions, significance, justification, scope, limitations and assumption of the study.

#### **1.2 Background to the Study**

Management of security of Information Technology (IT) systems remains a major challenge in organizations and universities globally and in Kenya. Recent concerns attribute IT security management not only to financial investment in IT security appliances, but also to the need for reliable ways of estimating both the prevailing, and improved levels of information security after the investments (Rabah, 2018). Information security metrics is a special type of measurement that is derived by analyzing and comparing an entity's state of information security to a predetermined implementation baseline of information security elements; whose measurements are taken over time (Tipton & Krause, 2000).

Elements of information technology security are the building blocks of robust and secure information systems that holistically constitute the parameters for managing IT security. Mitnick and Simon (2011) highlighted the major IT security elements as: security policies, physical security, network security, data security, and access control. Casey (2011) showed that information security metrics is generated from analysis and interpretation of data collected on

elements of information technology, as the data is believed to give direction on the levels of implementation and management of the elements of information technology security in a given institution.

Recently, there has been growing interest in information security metrics as a factor to consider in improving management of information technology security. While high investment and funding in IT security tools and appliances improve information security, Lingard, Wakefield and Blismas (2013) argued that with respect to common management principle, to ensure better management of information systems' security, measurability and knowledge of the prevailing status of information security could be more critical. Moreover, this argument is supported by SANS (2007), which stressed that information technology security status should be measurable through suitable metrics, so that security of the information systems may be known, predictable and properly managed. With regards to the arguments, financial investments need to be augmented with reliable IT security metrics to ensure proper management of IT security, and for determination of any security improvements achieved after such investments within universities.

### **1.2.1 The Dependency of Universities on Information Technology**

Today, universities all over the world rely on information systems or automating and creating efficiency in their administrative and academic operations. Internationally, US based universities find networked and automated information systems very important for both administrative and academic operations. Sekeres and Bevans, (2016) noted that most of the US-based universities have adopted financial information systems that ride on the networked infrastructure and singularly holds data for over 80,000 stake-holders, who are mainly the students and employees. The study explained that students' management systems and academics management systems are used to hold, process and transfer names, e-mail addresses as well as social security numbers of faculty members and students. Stojmenovic and Wen (2014), underscored that database systems containing campus records, dating back to many years of the institutions existence, have been created in the American universities. Moreover, automated information systems are used to process student performance results, staff credit management and fee collection for the students in US universities.

In the United Kingdom, many universities use examination management systems for capturing examination questions, generating sample examination papers and grading students' scores (Howe, 2015). This kind of system is not only vital in supporting the core mandate of the university, but also remains so sensitive that a lot of efforts must be put in place to secure it. Bevans (2016) showed that in some Australian Universities, SmartRider systems are used to automate payment of bus ride services. Critically, the system is managed by a rider-management application that is attached to the general information systems of the university through networked systems. This implies that any security factors affecting the critical information systems in the university impacts on the bus-management systems as well.

Most African universities have embraced information technology to major levels. Jaffer, Ng'ambi and Czerniewicz (2007) noted that e-learning platform systems which are attached to university websites are among the trending modes of learning in South African universities. The study reaffirmed that just like in the global universities, databases and application systems used for managing academic, financial, transport, examination and administrative functions are very important to the universities in South Africa. Apart from this, the executives of universities in South Africa apply automated information systems for strategic management of the institutions.

In Nigeria, Nweze (2010) underscored that the universities depend on computerized systems for managing academics, staff attendance, payment processing, borrowing of reading materials in the libraries, communication, internet based research and provision of security management systems like bar-code readers within the universities. Ugandan universities use information technology systems for examination management, grading, and administrative purposes, (Tibenderana & Ogao 2008). In Tanzania, the universities apply information systems to manage work flow, faculty administrative and academic functions as well as communication within the universities, (Luambano & Nawe 2004). The studies reveal the universities' continued dependence on information systems as well as the need for reliable management approaches for providing information security therein.

Universities in Kenya are increasingly embracing information technology to advanced levels. According to Makori (2013), information technology facilitates operations in the universities in Kenya in many ways, including: supporting academics, administrative and security functions. It observed that information technology facilitates handling of academic and administrative data at the levels of file generation, storage, processing, caching, long haul transit and transfers through local area networks - which in effect expose the university's data to cybercriminals and other online threats. Tarus, Gichoya and Muumbo (2015) revealed that the number of Universities in Kenya employing the use of enterprise resource planning (ERP) and other automation systems is increasing continuously. In addition, the use of ERP systems in institutions implies that there is system controlled work flow management for different divisions within the universities in Kenya. The work flow processes generate high volume of files that need to be kept safe.

Academic operations are currently being facilitated by information technology in the universities in Kenya, (Gichoya & Muumbo 2015). E-Learning systems are now at the centre of academic operations within both private and public universities in Kenya, thus calling for increased need for information technology security management among the universities to protect information residing in electronic form and in transit over the internet (Mingaine 2013). There is therefore, so much dependence on computerized systems in the universities that information technology security management needs to be considered further.

### **1.2.2 Information Technology Security Challenges in Universities**

Today, information technology systems for universities across the world experience security breaches. In the United States, Sekeres and Bevans (2016) noted that a hacker broke into the computer system of a university based in California and compromised data confidentially. Stojmenovic and Wen (2014) noted that systems for a university based in North Dakota was breached and used to attack other computers systems. The study noted that there was flat computer network, lack of intrusion detection systems, with little segmentations and inadequate firewall configurations. Stojmenovic and Wen further explained that the compromised information systems' security was attributed to the lack of monitoring systems for IT security status in the institutions.

In the United Kingdom, Howe (2015) showed that a 25 year old exam cheat was jailed for hacking into a university's computer system using a keyboard spying device “key-logger” to steal and use passwords of authorized entities in the system and upped five exam’s marks. In Australia, IT students were convicted for hacking and benefitting fraudulently from transport and bus ticketing system, (Bevans 2016). The studies point to an indication that internal attack on information systems is prevalence within universities are related to inadequate metrics to inform IT specialists and executives on the status of information security within the institutions.

In Africa, Jaffer, Ng'ambi and Czerniewicz (2007) noted that e-learning platform systems which are attached to university websites are mostly rendered unavailable whenever the university websites are attacked. Nweze (2010) showed that security breaches in computerized systems account for loss of investment in information systems in the universities in Nigeria. The study cited physical loss of IT facilities, system hacking, vandalism and theft of information systems' facilities as among the major challenges faced by the universities in Nigeria. In the year 2015, a Ugandan university was attacked and security of the information systems breached. According to (Tibenderana & Ogao 2008), a probe confirmed that more than 418 students managed to breach a university’s I.T security and altered their marks to better grades. The compromise of data integrity involved not only change of grades, whereby 62 students who were not eligible for graduation due to low performance still appeared in the graduation booklet.

In Kenya, Eira and Rodrigues (2009), showed that Kenya is among African countries leading in cyber-attacks, just like Morocco, Nigeria and South Africa. According to Mingaine (2013), the universities in Kenya are rich targets for hackers who gain unauthorized access to compromise academic and financial data in the institutions. According to Mang’ira and Andrew (2014), in the year 2011, all Kenyan public universities’ managements were cautioned against a group of university students that was hacking into computer systems of both private and public universities and compromising the academic and financial data integrity. Okibo and Ochiche (2014) noted that employees and students of another public university in Kenya hacked into the university’s database, using online techniques and compromised its integrity by altering examination results in the year 2011, thus affecting graduation that had been scheduled.

Mang'ira and Andrew (2014) highlighted that the availability of information systems' resources in universities in Kenya is affected not only by hacker activities, but also by physical security incidents like natural disaster, accidental and deliberately actions, including disconnection of network cables, computer theft, vandalism, floods, sabotage, fire, strikes/riots and lighting.

In all the universities above, the studies reported computer theft, cut on data cables, vandalism of information facilities, and unaccounted for portable wireless devices which could affect availability of information resources within the universities were reported. Further, they indicated that weak information security practices, low levels of implementing physical security controls around IT facilities, inadequate data security provision, non-implemented information security policies, little network security and uncontrolled access to the university systems had a bearing on the reported breaches. Despite these vulnerabilities to information systems, the studies showed lack of suitable information technology security metrics and measurement approaches within the institutions.

### **1.2.3 Metrics Factor in Information Technology Security Management**

According to Tipton & Krause (2000), information technology security management refers to the practice of coordinating activities, regulations and operations that direct and control the preservation of confidentiality, integrity, and availability (CIA) of information asset. As supported by (Calder & Watkins 2008), that since it is difficult to manage what one cannot measure, information security management using appropriate metrics is necessary within organizations and universities.

### **1.2.4 IT Security Metrics**

Metrics has attracted different but related definitions across different fields. In mathematics, for instance, a set metric is defined as a function of distance that describes the physical space between each pair of elements of a set, and thus shows how far an element is with reference to a given standard point, (Toth & Vigo, 2014). In control systems, it means a number of universal standard inputs which are chosen as reference, against which other measurements are considered when designing a system, (Boyer & McQueen 2007). In social sciences, it is

argued that for one to gauge the personal well-being and to make further progresses, life metrics for measuring success are necessary. Moreover, entrepreneurs use product life cycle metrics to estimate the performance levels and progresses made in business, (Stark 2015).

In strategic management field, metrics are perceived as measurements that are derived from the line of key performance indicators (KPIs). With regards to this view, Mingaine (2013) showed that a metric constitutes a statistical approach which gives a measurement of an organization's overall performance with reference to data collected from the PKIs. In the field of informatics, Lukman, Krajnc and Glavic (2010) explained webo-metrics ranking of universities as a measurement system for indexing the universities based on a combination of key performance indicators (KPIs), like the website contents, the visibility, hit-rate and impact of these elements as perceived through external hyperlinks

The above studies converge to a sense and recognition that metrics not only help in establishing the situation as it is currently, but also informs the basis for any improvements that are possible, as well as quantifying such improvements once an IT security improvement project has been undertaken - an understanding supported by (Calder & Watkins 2008). Further even though the studies' definitions of metrics vary slightly with respect to their unique fields, they all converge to the point that metrics are special types of measurements, which derive data from key performance indicators (elements), and apply statistical techniques on the data to give accurate status in relation to performance levels of the elements. However, IT security metrics models are still inadequately addressed. In analogy, when metrics are applied to information security field, the elements of information technology security are considered as the key performance indicators, which should be analyzed through relevant statistical techniques, to give a picture of information technology security status.

### **1.2.5 The Elements' Factors in Information Technology Security Management.**

Sekeres and Bevans (2016) studied the information technology security breaches in the university based in California and the possible factors which could have contributed to the reported breaching of the information systems' security. Along the elements of IT security, the

study noted that flat computer network, with little segmentations and inadequate firewall configurations was associated with vulnerabilities that made the attack successful. The information systems' security lapse was attributed to the ease of attack on the systems. Since the technical staff admitted lack of user-groups, segmentations and required levels of firewall configuration, adoption of check points for security status was recommended to provide proactive approach to security management, (Bevans 2016). In the study, information security metrics emerged as a required approach for better and proactive information security management.

Stojmenovic and Wen (2014) noted that systems attack for a university based in North Dakota could have easily been reduced if basic level information security metrics systems were in place to alert the systems administrators of areas associated with vulnerabilities. The study asserted that since university information security covers wide areas with multiple elements, use of information technology security metrics to give a close picture of information technology status related to the major elements can be an asset for information technology security management.

According to Gritzalis, Kandias, Stavrou and Mitrou (2014), information systems for some universities in Texas were victims of malicious systems attack that compromised the security of critical databases for students and administration. The study reaffirmed that in most cases of breaches of information systems' security, the colleges' administrations admitted that the situation could have been avoided through basic assessment of information security vulnerabilities and security status checks prior to the attack. It is against this backlash of proactive information security management that poses emphasis on the need for information technology security metrics, based on network security and access control, as a tool for better management of information technology security within universities.

Even though the use of passwords had been adopted for controlling access to information systems in universities in the United Kingdom, Howe (2015) noted that administrators could not make early detection of a possibility of students using administrators' password to gain unauthorized access and manipulate examination databases. Since the security levels of databases bearing examination files were not clear, the study explained that improvements made

through investing on data security could not be quantified either. This highlights the requirement of security metrics related to data security for better management of data security in universities.

Further, in South Africa, Jaffer, Ng'ambi and Czerniewicz (2007) elucidated that since weak information security practices, low levels of implementing physical security controls around IT facilities, inadequate data security provision, non-implemented information security policies, little network security and uncontrolled access to the university systems are attributed to information systems' security breaches, ways of measuring security status along the highlighted areas ought to be adopted to make security management in universities easier.

Analyzing security breaches for computerized systems in Nigerian universities, Nweze (2010) pin pointed inadequate adoption and implementation of IT security policies, lack of physical barriers, porous network and little data security practices as possible contributing factors to information security breaches. However, the study highlighted inadequate ways of monitoring information security levels along the mentioned lines of system security and recommended the need for IT security metrics for better management of IT security within the universities.

Weak policies for controlling access to the computer information system, little controlled physical access to computer facilities, unsecure examination databases and risky practices around the use of passwords were associated with systems vulnerabilities within universities in Uganda, (Tibenderana & Ogao 2008). The study suggested adoption of information technology security metrics as a possible effective way to improve information systems' management within the universities. It's arguable that such metrics allow proactive monitoring and detection of vulnerabilities along the major elements of IT security, that if strengthened would timely reduce the vulnerabilities, could make IT security management more effective.

In Kenya, Mang'ira and Kitoi (2011) attributed loss of physical computer devices, vandalism, and theft and fiber optics line cuts to inadequate IT security metrics that show the levels of physical security implementation in universities in Kenya. It argued that while availability of inventories, signage that identifies critical computer assets and areas traversed by data lines is necessary, a status indicator approach relating the required number of signage and other physical

security practices against the available number already installed, is necessary for managing IT security within the universities. In support of this view, Okibo and Ochiche (2014) indicated that for access control to information systems in universities in Kenya, standard elements of access control should be established, and then compared with the already existing access control mechanisms, to help establish information security status within the universities. This comparison not only gives picture of the levels of implementation of the security interventions for information systems, but also portrays the additional efforts that need to be undertaken to improve IT security. Ndung'u (2015) study on enterprise resource management - ERP, revealed that ERP associated systems security challenges within universities in Kenya are attributed to lack of security monitoring tools as part of information systems security management.

There is increasing admission by systems' administrators that most of the information system security breaches experienced within universities in Kenya can be minimized if reliable metrics were in place, to provide proactive security management, (Bichanga & Obara 2014). In support of this, Stojmenovic and Wen (2014) found that reliable IT security metrics has statistically significant relationship with effective management of information systems' security.

In a synopsis, with reference to the aforementioned studies on metrics, and Tipton & Krause (2000) definition of information security metrics as special type of measurement that derive data from implementation levels of key performance indicators KPIs (elements if IT security in this case), and apply statistical techniques on the data to give accurate status and performance levels of the elements; whose output is a measurement of the organizational IT security situation / or levels. The universities' information systems security continuously get compromised since its management lack appropriate metrics model developed from this vital relationship. A gap therefore exists wherein the relationship between the levels of implementation of the KPIs (the IT security elements) and the metrics has not been adequately established in the universities.

### **1.3 Statement of the Problem**

In this study, the problem was lack of reliable IT security metrics model for proactive and continuous monitoring of systems security in universities in Kenya. Most universities in Kenya

lack adequate IT security metrics, yet such metrics is a vital component for proper IT security management. Some of the current information security measurement approaches used in the universities include; intuition - whereby security metrics are based on the users' dynamic personal feelings, the number of onslaughts on information systems, as well as types of security tools' appliances deployed in the infrastructure.

IT security metrics should be measurements based on the levels of implementation of IT security elements in the entire infrastructure. The issue of lack of reliable IT security metrics and model in the universities is a problem of great concern because if an organization cannot measure its IT security status, then it cannot properly manage it properly. The gap in knowledge is the relation between IT security elements' implementation levels and measurement of IT security levels. Establishment of this relationship can be useful in developing metrics for proactive management of IT security. Studies in the background section above showed that many cases of system security breaches which affected universities' stakeholders were attributed to inadequate metrics. Consequently, poor management of IT security is related to vulnerability of the entire information asset which contains critical information affecting the university students, administrators and other stakeholders.

If this problem is not addressed, then inappropriate metrics will continue to be applied in the universities' information systems. This can result into continued poor management of information security, bearing further risks of breaching confidentiality, integrity and availability of critical information for universities' stakeholders. Development of IT security metrics model based on implementation levels of major elements of IT security had not been adequately explored. This study sought to investigate the major IT security elements, developed the security metrics' model statistically based on the implementation levels of major elements of IT security; a model that not only establish IT security status, but also provide continuous security monitoring. In addition, the study tested the applicability of the model in estimation the prevailing IT security status for universities.

#### **1.4 Purpose of the Study**

The purpose of this research was to investigate the major elements in IT security management, determine the elements' relationship with IT security measurements and to develop and test a suitable IT security metrics' model for universities in Kenya.

#### **1.5 Objectives of the Study**

The study was guided by the following objectives;

- i. To investigate the major elements for IT security management in universities in Kenya.
- ii. To determine the relationship between implementation of the major IT security elements and IT security measurements in the universities in Kenya.
- iii. To develop suitable IT security metrics model based on implementation levels of major IT security elements for universities in Kenya.
- iv. To determine the applicability of the developed IT security metrics model for universities in Kenya.

#### **1.6 Research Questions**

The following were the research questions for the study,

- i. What are the major elements in IT security management in universities in Kenya?
- ii. What is the relationship between the major IT security elements' implementation and IT security measurements in the universities in Kenya?
- iii. What is the suitable IT security metric's model based on major IT security elements' implementation for universities in Kenya?
- iv. What is the applicability of the developed IT security metrics' model for universities in Kenya?

#### **1.7 Justification / Significance of the Study**

In Kenya, Kitheka (2013) criticized the current reliance on personal feelings to estimate IT security status within universities, and recommended the use of approaches based on IT security elements as suitable. Ndung'u (2015) revealed that the daily ERP systems security attacks within universities in Kenya could be attributed to inadequacy of security monitoring tools, and pointed

to suitable metrics as a necessary part of effective information systems security management. Mang'ira and Kitoi (2011) attributed loss of physical computer devices, vandalism, and theft and fiber optics line cuts to inadequate IT security metrics in universities in Kenya. The study is therefore necessary because, while attacks on universities' information systems occur quite frequently, most of the security breaches could be limited if suitable IT security metrics and monitoring systems were in place.

A research on information technology security metrics approach based on major IT security elements, had not received much academic focus within the universities in Kenya, despite several studies' affirmation of positive relationship between the metrics and effective management of IT security. The resultant functional model can benefit university stake-holders to enhance system security management through measuring prevailing IT security levels.

### **1.8 Scope of the Study**

The research was conducted to investigate the application of major elements of IT security in managing IT security within universities in Kenya and developing a suitable IT security metrics' model. The study covered IT security implementation levels and measurement in the perspective of major elements from selected Kenyan universities' systems administrators and users. Statistical analyses including mean and regression were employed and used in developing the resultant metrics model. The study however, did not cover the application of digital sensors for automatic data input into the model.

### **1.9 Limitations of the Study**

The potential weaknesses identified in this study include: the study was limited to the universities in Kenya due to resource constrains, and as such, the findings may not be generalized to other institutions of higher learning. The limits associated with statistical analysis approaches based on regression, goal-question metrics, could only determine correlation between the major IT security elements and metrics, but not causation aspects of the variable; the inaccuracies inherent in goal-question metrics method, which is characterized by laborious expert estimation for preparing detailed goals, the corresponding questions and answers, as well

as setting weight for every element of IT security. Also, sample size of about ten percent is a limitation since ideal sampling should include the entire population.

In overcoming the inherent limitations: sample size provided characteristic information about the population due to homogeneity of operations in private and public universities. Further inclusion of purposive sampling ensured that many operation areas were covered to get more characteristic data of the population. The statistical analytic limitations were overcome by introduction of error term (E) in the model equation, which was used in the model's model.

### **1.10 Assumption of the Study**

The researcher went into this study with an assumption that all universities in Kenya have attained appreciable levels of computerization, that the networked computerized systems are currently used for academics and administrative functions, and that the dependence on computerized systems within universities will continue even in future. This was a suitable environment for this kind of study. Indeed, the research found that all the universities had adopted appreciable levels of computerization in their operations, which made the research feasible.

## **CHAPTER TWO**

### **LITERATURE REVIEW**

#### **2.1 Introduction.**

This chapter focuses on the general overview of literature related to the main concepts, the role of standards in IT security metrics and management, and Goal - Question - Metrics (GQM) concept. Further, the section covers colour codes concept for general security metrics, IT Security metric's dashboard and the elements in IT security management in universities. In addition, the gaps to be addressed, conceptual framework, as well as relevant theories are reviewed.

#### **2.2 General Overview of Literature Related to the Main Concepts**

This section covered the general literature related to the main concepts including the role of standards in security metrics and management, the goal-question-metrics (GQM) concept, the metrics presentation approaches of colour codes and dashboards.

##### **2.2.1 Role of Standards in IT Security Metrics and Management**

Jansen (2010) explained that international IT security standards are the criteria for best-practice information security management, which provides comprehensive specification for ensuring information security under the principles of confidentiality, integrity and availability. The standards provide a set of best-practice controls that when applied to an organization's information infrastructure in a structured manner, not only enhances data security, but also achieves externally assessed and certified security compliance.

Development and sustainability of a good information security management system within organizations has been guided by information security standards like ISO 17799, ISO 27001 and

ISO 27002, (Calder & Watkins 2008). The standards indicate best practices, which allows gap-analysis and hence may be used in determining the status of information technology security implementation in universities (Ismail & Zainab 2011). The standards exist in their generic form, and must be customized to benefit university IT environment. Therefore, many of the organizations that have adopted the standards have customized the international IT security standards for their internal use. According to Arnason and Willet (2008), some of the standards applied in most institutions include ISO/IEC 27001), ISO/IEC 27002, COBIT and (NIST) 800. However, Calder and Watkins (2008) revealed that most institutions of higher learning adopt a hybrid of both requirements for COBIT and ISO 27001 / 27002 as they are more comprehensive.

Whitson (2003) studied the model of CIA triad as applied in information security management within Australian universities in relation to IT Infrastructure Library (ITIL). The model, as the study showed, guarantees confidentiality, integrity and availability of information if implemented according to the standard. However, the levels of IT security implementation portrayed a deviation from the standards. It further revealed that the institutions used the criteria set by the standards to gauge the status of information security. This is an indication that IT security standards could be relied upon to provide bench-marks for setting up IT security metrics. On the other hand, Jansen (2010) analysed the provision of IT security metrics using special NIST standards as the guideline, and showed that the CIA model of information security management as proposed in Whitson (2003) is inadequate, as it did not factor in accountability and responsibility features and hence a better security management and measurement model for information systems ought to be adopted.

Casey (2011) stressed that since achievement of information technology security is made mainly through implementation of: security policies; risk analysis; IT security procedures; proper documentation; providing training & awareness; and data recovery. IT security standards that guide the mentioned features of IT security could provide the scope for reference in measuring IT security status. This study agreed with Anderson (2001) that argued that for development of suitable IT security metrics, inclusion of IT security elements' according to IT security standards requirements is necessary within universities. As discussed earlier, May (2003) recognized the role of information security standards on metrics in facilitating improvement of IT security

management within Australian Universities, and in agreement with Lane (2007), stressed that information technology security can be well managed if measurement of the status is possibly guided by performance along the major elements of IT security.

Mahnic, Uratnik and Zabkar (2002) studied information systems security among Slovenian universities and concentrated on the application of COBIT and BS 7799 as benchmarking standards. The study concluded that university academic and financial information systems had much high levels of security as compared to other information systems, and revealed higher levels of compliance with COBIT in practices around the financial and academic information systems. While the study showed IT security requirements of the two standards, it indicated that more still needs to be explored in relation to the standards' application to measure the information systems security in the Slovenian Universities.

In South Africa, Mohlabeng, Mokwena and Osunmakinde (2012) undertook a research to investigate the implementation of information technology security strategies based on NIST, within higher education institutions. According to the study, among the elements of information security to be considered in the management framework are IT policies, users, network, and the general IT infrastructure security. While this suggestion concurs with Jansen (2010), which showed that holistic framework - including all major elements of IT security can offer better security management for IT systems, it found out that IT security practices in the institutions did not meet international standards. This implies that the systems still had inadequate IT infrastructural security. Compliance with standards could improve not only the IT security, but also IT security metrics based on the international IT security standards' requirements along the major elements of IT security.

In Kenya, Mingaine (2013) studied the information security management systems in Kenyan public universities, and looked at a gap analysis between common practices within the universities against best practices based on international standards for IT security in the industry. Also, the study sought to determine the factors influencing effectiveness of information systems security management within the universities. It established that even though the institutions mention COBIT, NIST Special Publications and ISO 27001 as the guiding standards for IT

security, the actual IT security practices around the elements of IT security do not conform to the requirements of the standards. The study showed that the gaps were varying from one university to another, but the accurate levels of the gaps / deficiencies were not explored. The study however, showed that the standards could be relied upon to generate guidance on the parameters for IT security metrics for universities. The study further suggested that analysis of the gap between the practices around elements of IT security when compared to the standards' requirements can be used to establish IT security status, and thus provide a platform for monitoring IT security implementation levels based on the elements of IT security.

## 2.2.2 International Organization for Standardization (ISO) 27001

The ISO 27001 international standard defines the scope of obligatory requirements for general information security management system. Lodgaard and Ashland (2011) found that the standard considers major IT security elements in the management model and can be applied to help manage information systems' security. However, Johnson (2002) showed that ISO 27001 standard in the entire "Plan- Do-Check- Act" (PDCA) as a tool to manage information security, is lacking on how the IT security elements can be applied in measuring IT security levels.

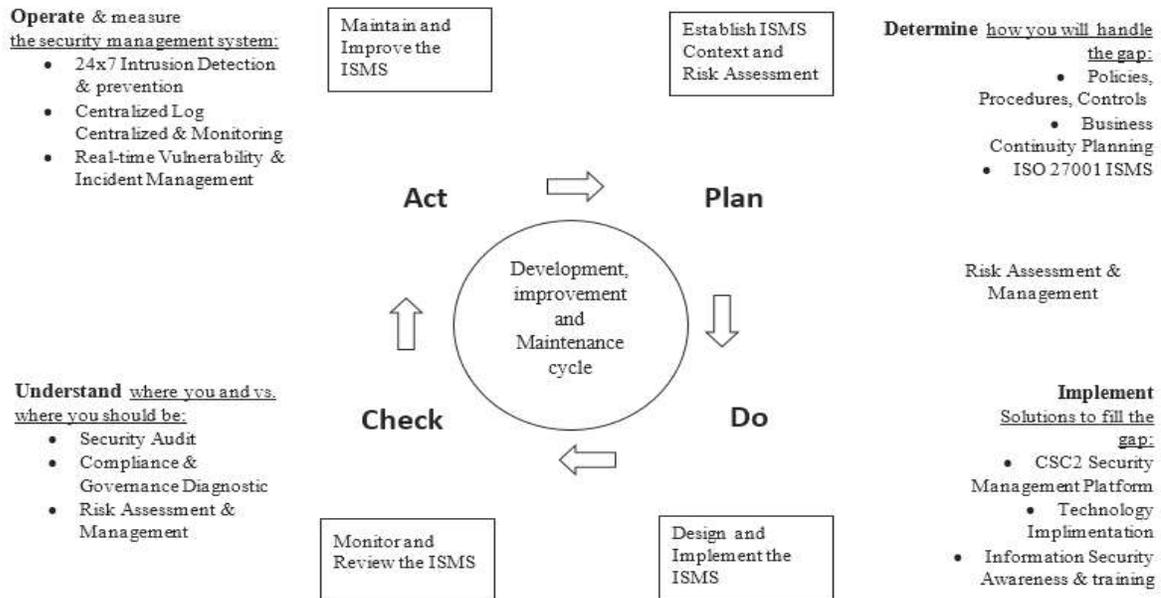


Figure 2.1: Johnson's PDCA Quality Progress chart Source: Rajiv, (2009).

## International Organization for Standardization (ISO) 27002 Standards

According to Briggs, the ISO 27002 defines a detailed set of information security controls with best-practice security objectives that specifies the requirements for establishment, implementation, operation, monitoring, review, maintenance and improvement of documented information security management systems. However, Fenz, Heurix and Neubauer, (2015) noted that both ISO 27001 and ISO 27002 give comprehensive IT security requirements, but have not addressed metrics concerns of information security in the universities.

### 2.2.3 Control Objectives for Information and Related Technology (COBIT)

COBIT is an IT security management framework that was developed by Information Systems Audit and Control Association (ISACA) in conjunction with the information technology governance institute (ITGI) around 1992. In the University of Applied Sciences North-western Switzerland, a review by Pasquini and Galiè (2013) found COBIT to be a supporting toolset that helps information technology managers to bridge the gap between technical issues on IT security control requirements, and inherent business risks.

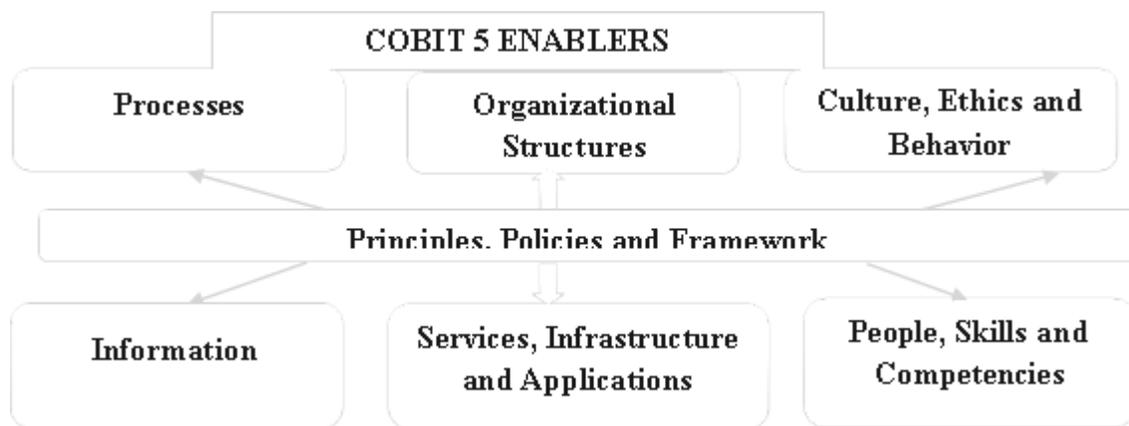


Figure 2.2: Cobit 5 Enablers: Source: Pasquini and Galiè, (2013),

A study by Leiden University researchers in the Netherlands examined the effectiveness of COBIT framework in the organizations' IT departments. According to Zhang and Fever (2013), proper implementation of COBIT frameworks reduces IT security gaps and improves safety of

information in the Netherlands. In Qatar, a Carnegie Mellon University researcher did comparison between COBIT and ISO 27001 / 2 and found that the two standards when used together cover the major elements of IT security. In a similar study conducted within Carnegie Mellon University in Qatar, Arora (2010) findings recommended direct mapping of COBIT and ISO 27001 / 2, hence showing that the two standards can be used to complement each other when managing information technology security in universities. Arora noted that COBIT's main weakness is that it lacks models to address specific key elements of IT security such as the server security, network security, application security and database security.

In the universities where it is applied, COBIT provides guidance on Information Technology governance and risk management in general, which constitutes the responsibility of the top management of the university, and involves leadership, structures and processes to ensure the university's information technology sustains the organization's core business strategies and objectives, (Calder & Watkins 2008). In a similar study done in the Iranian university, Sheikhpour and Modiri (2012) concurs with Arora (2010), that COBIT and ISO 27001/2 can be mapped into each other for better information systems' security management, and further developed a framework to map COBIT control processes into the ISO 27001 managements controls for information system' security. The resultant framework however did not show ways of using the IT security parameters towards creation of IT security metrics.

However, among universities in Kenya, Mong'ira (2011) reviewed the standards and revealed that information technology security requirement at the metrics levels are not addressed directly by both standards, but innovation around the provisions in the standards could be used to yield a metrics approach based on the levels of implementation of the major elements of IT security. In summary, international IT security standards could be used as a criterion to gauge the status of information security implementation levels within universities. This is an indication that IT security standards could be relied upon to provide bench-marks for setting up IT security metrics. However, more still needs to be explored in relation to the standards' application to measure the information systems security, as the standards are lacking the direct approaches in measuring IT security levels. This calls for an innovative approach to derive suitable measurement for IT security status, as guided by the standards and based on the major elements

of IT security. ISO 27002 is a holistic managerial approach to information technology security, which considers most elements of IT security.

On the other hand, COBIT does more in aligning IT security practices to the core business of the organization. COBIT's main weakness is that it lacks models to address specific key elements of IT security such as the server security, network security, application security and database security. Therefore, when COBIT and ISO 27001 / 2 standards are used together, they cover the major elements of IT security that are necessary for metrics development, and also directs IT security practices to align with the core objectives of the organization. The standards' major role in IT security metrics is the definition of the bench-marks for the requirement of IT security along the lines of major elements of IT security. The IT security status therefore, is perceived as the relationship between the levels of implementation of security features on the elements of IT security, against the standards' expectation.

In summary, studies around the aforementioned security standards showed bench-marks for information systems' security implementation which helps to reveal the gaps from one institution to another, but the accurate levels of the gaps / deficiencies were not explored. The standards however, do not provide means of establishing the prevailing information systems' security status based on the implementation levels of major elements of IT security.

#### **2.2.4 Goal - Question - Metrics (GQM) Concept**

(GQM) is an acronym for “goal-question-metric” paradigm that has been used for a long time to support the application of quantifiable data grounded on goals into easily interpreted measurements, (Macrae 2003). GQM was originated by Victor Basili and D.wiess in 1980's. A researcher, like D.rombach found the GQM concept viable in solving measurement problems in a practical way. In software industry, for instance, Jordan, McMahan and Panlilio (2005) demonstrated that GQM can be applied as an approach for deriving metrics for software productivity from a set of data related to software development, the product quality and it's utility. In conclusion, the Basili and Wiess study showed that apart from the field of software

development, GQM is easily coordinated with the environment of any organization; hence it could also serve as base framework for IT security measurement initiatives. In support of this,

Ampatzoglou, Ampatzoglou, and Avgeriou (2015) found that when applied in such initiatives, it allows achieving reliable metrics regarding the organization's IT security implementation levels and practices which can be applied as benchmarks for IT security improvement and maintenance. Further, Vaishnavi and Kuechler (2015) showed that GQM method can be used as measurement framework to measure the prevailing IT security status and to inform the improvement direction that could be adopted. Vaishnavi and Kuechler further explained that operational level involves the routine activities that are involved towards establishment, implementation and maintenance of IT security within an organization. In this level, there are set of questions that are related to the operations and are hence used to specify the models in object.

### **2.2.5 The GQM Step in Metrics' Modeling Process**

According to Mashiko and Basili (1997), the step process in GQM is as follows:

#### **Step one**

This involves the development of IT security goals and related measurement at the objective's levels. In this research, initial step included the relative approach to determine the extent to which elements of IT security are implemented in the organization. This was done by considering not only the broad category of the elements, but also the sub-elements therein at the operation levels.

#### **Step two**

This involves generating questions on the IT security goals to help in defining the goals completely and in quick, coherent manner that ultimately prompts answers which show the extent of implementation of the IT security elements in the organization.

### **Step Three**

This involves specification of measures in form of ratios or percentages indicating the levels of achievement of the goals in relation to the expected conformance for specific goals.

### **Step Four**

Here, mechanisms for collecting, validating and analysing the data on the performance of the elements of IT security in the organization were developed. In this case, both objective and subjective contents come to play in analysing the collected data in real time to provide feedback on the performance of the elements of IT security. For this research data came from information systems' experts and users who are well conversant with the given organizations' IT systems in their respective docket. This approach gives room for both the objective and subjective factors to play roles in shaping the metrics' output.

### **Step Five**

The fifth step involves statistical analysis of the data, through the application of regression model which is conducted using computer codes, and then the result, becomes a summarized output of the data analysis. This output constitutes the overall metrics, which can be displayed in IT security dashboard, and mapped on the various colour codes for easy interpretation.

Murugesan and Gangadharan (2012) applied a similar GQM model for metrics, and analysed the advantages of GQM as follows: GQM approach helps in understanding, managing and monitoring the organization's IT security practices in relation to the elements of IT security. Further, it is important for certifying and judging the improvement activities on IT security investments. However, the major disadvantage of this approach is that selection of metrics and quality attributes could be subject expert judgments.

## **2.2.6 Colour Codes Concept for General Security Metrics**

The colour - codes for IT security situation awareness can be used as a system for conceptualizing the behaviour pattern of information systems owners at different circumstances, Schwartz (2010).

Thomas *et al.* (2015) asserted that there is no better self-communicating metaphor for creating the awareness state of mind than by the use colour code scheme, but with exception of colour-blind people. Many information systems end up in risk situations since majority of those in charge do not see the danger or threat in advance before it becomes a serious problem (MacLean, 2012). Information systems security situational awareness is the ability to scan the systems environment and sense security challenges and opportunities, with minimal interference caused to the normal operation of the system (Furnell, Bryant & Phippen 2007).

According to Krombholz *et al.* (2015), IT security situation awareness constitutes at least 90 percent of proactive security management. This kind of view was supported by MacLean (2012) which showed that being aware of the prevailing IT security situation, system administrators can identify and avoid potentially dangerous information system situations. The concept of colour code for evaluating security situation awareness was first developed by Jeff Cooper during the Second World War. Colonel Jeff Cooper's security situation analysis and demonstration using colour codes was successfully applied to create an awareness system that associated levels of security risks to specific colors, (Angelini & Santucci 2015). According to Lenders, Tanner and Blarer (2015), by understanding how data collected from the IT security elements can be processed to indicate levels of danger.

### **2.2.7 Colour Codes in IT Security Management**

Colour codes scheme has been successfully applied in the field of information technology to show the levels security status and implementation levels of the elements of IT security. Angelini and Santucci (2015) demonstrated that a visual cyber situational awareness creates proper proactive security management technique for critical systems' infrastructures. It argued that cyber management space security for an organization could be improved when colour codes are used to show the security status of the systems at any given time. Lenders, Tanner and Blarer (2015) supported this argument through further demonstrating gaining an edge in cyberspace security management through the application of an advanced situational awareness colour-code scheme.

Similarly, Thomas *et al.* (2015) showed that there could be substantive reduction in access control vulnerabilities through the use of interactive colour code annotations that provide earlier warnings to IT security experts. Furnell, Bryant and Phippen (2007) assessed the IT security perceptions of personal internet users and concluded that the majority would feel safer when browsing through URLs shaded green.

### 2.2.8 Metrics Presentation in Colour-Codes

According to Trethowen, Anslow and Welch (2015), the measurements' outputs should be related to colour codes for better visualization. The idea for better visualization is further supported by (Kruger and Kearney, 2006). Therefore, measurement from a metric's model should be categorized into three, depending on the magnitude, and then mapped into corresponding colour codes associated with the different security status as shown below. Red implies severe security status that needs immediate attention, and it takes measurement values lowest in the scale. Yellow means insecure environment that needs consideration for improvement and takes middle -ranged values, while Green means a safe computing environment that needs to be maintained and takes the highest values in the scale. The actual scale values were derived through statistical computation in the results' section of chapter four.

Table 2.1: Conceptualized Metrics' Presentation in Colour-Code

lowest scale		
Severe security status <i>(Needs immediate attention)</i>	Insecure <i>(needs improvement)</i>	Safe <i>(Needs maintenance)</i>

Source: The researcher, .2018. As adopted from chapter four.

### 2.2.9 IT Security Metric's Dashboard

ICT staff members make so much IT security observations from their daily operations in different organizations. Some of the observed elements could contribute tremendously in improving ICT security if presented before management for consideration. However, according to Beas and Salanova (2006), most ICT personnel hardly express and present the observations in

a manner that the executive can understand and consume towards bettering IT security. This implies that once the observations related to IT security have been made, they need to be recorded and displayed in a format that the organizations' management and the general stakeholders can understand and consume easily.

According to Thornton (2001), a picture is worth more than a thousand words when used in communicating technical issues. This implies that a complex technical idea can be passed more effectively across a multiplicity of audience, by using a single still image than a using a long narrative description. While this notion is supported by other studies including Safer (2012) on marine performance as seen on pictorial logs, Roth and Bowen (2003) showed that when graphs are used in communicating technical information, it becomes more effective than the use of ten thousand descriptive words. On the other hand, Ballou, Heitger and Donnell (2010) demonstrated that creating effective dashboards involves incorporating both pictorial and graphical features for clear illustration and visualization. This implies that pictures and graphs should be used together to constitute a dashboard that ultimately communicates technical information in an IT security set-up.

In information and communication technology, a dashboard is a graphic user interface that, operates like an automobile's display, which organizes and presents information to the driver about mileage, speed, fuel levels, transmission and other information related to the machine in a way that is easy to read and understand. Dashboards have been applied in a number of fields, including information technology, to help present information more effectively than when using long descriptive narrations. The use of dashboards has helped to establish accountability across various project activities, automate performance reporting processes, provide methodological support based on given pre-defined computer programs, and to enable business consequence modeling for real-time reporting of performance levels, (Haubner & Petermann 1986)

Filonik *et al.* (2013) successfully demonstrated a customizable dashboard display used for environmental performance and visualizations. This made communicating technical issues of the environment to various audiences more effective as compared to the use of long descriptive narrations. Similarly, Elias (2011) applied dashboards in learning analytics and found it to

effectively communicate technical aspects among college students. Suakanto, Supangkat and Saragih (2013) modeled a smart city dashboard for integrating the various computer network related data for sensor networks, which demonstrated an effective illustration of performance. Ballou, Heitger and Donnell (2010) created effective dashboards and showed that it could be used by companies to improve executive decision making and board oversight. In addition, Walther, Slovacek and Tidwell (2001) showed that dashboards based on photographic images are really effective in long-term and short-term computer-mediated communication.

### **2.3 The Elements in IT Security Management in Universities.**

An element is generally understood as an important basic component of a complex object that constitutes it. For example, the components of an information system are regarded as its elements. In a study designed to measure the effectiveness of information security awareness program within selected universities in Germany, Veseli (2011) suggested that elements of IT security should be drawn from the major operational features of robust and secure information systems programs, along which effective management of IT security is executed. Veseli arrived at this conclusion after his analysis revealed that management of IT security becomes more effective if it is focused on the functional features of information systems. The study explained that even though there are many features of an information system, areas that are mostly targeted for security management, for example the networks, users' control, policies and databases should form an integral part of IT security elements.

Casey (2011) evaluated information security elements in the international scope and attributed them to three broad categories that are: technology, processes and people. This broad categorization of elements of IT security was supported by Martins, Eloff and Park (2001). In addition, Martins, Eloff and Park reviewed the broad categories and showed that they could be cascaded into major elements that reflect the operation areas on an information systems' infrastructure. Consequently, it contended that the major elements of IT security should include: security policies, physical security, network security, data security, and access control. Also, while partially agreeing with the two studies, Veseli (2011) suggested that the elements of IT

security should include further attributes like the aspect of people, malware, political factors, environmental issues, and security awareness among others.

Jonsson and Pirzadeh (2011) study on a framework for IT security management based on systems operation attributes in the realms of information systems' security, reviewed the metrics' structure used in universities in Sweden. The study analyzed operations areas within a robust IT infrastructure in universities, and highlighted the areas as IT department leadership, network section, database section, IT security, system administration as the major IT operation areas for IT administration and further showed that metrics should be derived along the operation lines of IT, like networks, databases, policies and access control. This implies that the security factors related to the operation features of information technology should constitute the elements of IT security. Tarus (2015) noted that students' finance, students' registration, examinations, human resources, internal audit, library, and computer laboratory are the operation areas of IT systems in the universities in Kenya. This view was supported by Ndung'u (2015) study indicated that most staff members in the operation areas have embraced information technology and use it at their places of work.

Similarly, Broadbent (2007) argument resonates with two studies, that including security elements of IT operational parameters like physical security measures, systems' access control, IT security policies, data security and network security can highly improve information systems security management in an organization. Also, Casey (2011) revealed that the use of reliable IT security metrics, rooted on the above elements of IT security can significantly improve IT security management within institutions. This approach helps to reveal the entire IT security implementation success levels and expose the areas associated with vulnerabilities, so that if these areas are focused on, dealing with them would mean high success levels in managing IT security. It suggests that universities should develop programs for monitoring and evaluating information technology security in relation to the security performance indicators, in order to improve IT security management.

In a synopsis, the foregoing discussion indicates that IT security is a broad field classified into people, processes and technologies. The major elements emanating from the broad categories

include security policies, physical security, network security, data security, and access control, users, malware control and governance of IT systems.

Since the elements belong to the three broad categories of; people, technology and processes, they directly contribute to estimation of operation levels in the general IT infrastructure and IT security as well, thus making them all significant. The researcher considered the similarities, the convergences as well as the controversies around the subject of information technology elements in the perspective of the studies to further investigate the major elements of IT security. In analysis, the preceding studies highlighted mainly the security policies, physical security, network security, data security, and access control as the major elements of IT security.

### **2.3.0 The Major Elements of IT Security Management**

When considered under operation levels, the broad areas under IT security composed of people, processes and technology are considered to be constituted by the major elements of IT security as: physical security measures, IT security policies, network security, data security and systems' access control, (Broadbent 2007).

#### **2.3.1 IT Security Policy**

Bulgurcu, Cavusoglu and Benbasat (2010) explained that IT security policy being a management document that provides super control over all the operational elements of IT security, should be viewed as an information systems' governance element that forms an integral feature of IT security. The study explained that institutions that employ IT security policy have greatly improved the confidentiality, integrity, and availability (CIA) of data and resources. It showed that when IT security policy is applied to users, it has the effects of directing resources available for the various user groups, as well as the time period when they can access the given resources. While Peltier *et al.* (2005) agrees that a well written security policy forms the cornerstone of an effective information security structure, the study illustrated that the policy introduces long systems' access and utilization procedures that may cause delays when serving the clients, especially student and other university staff. It argued that since IT security and resulting efficiency obtained from application of information systems needs balance, over-implementation of IT security policy could affect - availability, which is a core concern of IT security.

Within African context, Jagadeeshwar, Shriramoju and Babu (2016) attributed malware infestation within universities in Ethiopia to the increased use of mobile computing devices. The study claimed that effective information security policies have coped with malware infestation in the university. It further successfully confronted malware menace in private university in Uganda, and devised the use of IT security policy as a non-resource intensive way of controlling malware within a university. The study explained that since IT security policy implementation is not resource intensive, little investment through dedication of time and adherence to the policy could limit malware effect on information systems. Similarly, Sandvik (2016) found that malware causes multiple losses to information resources and it is a major contributor to system unavailability within learning institutions in Rwanda. It noted that apart from the use of anti-malware, like anti-virus systems, well implemented IT security policy, especially on user training helps in managing malware.

In South Africa, malware's adverse effects within institutional information systems' infrastructure raised much concerns to the extent that a supervised comparative study and analysis of attack methods for malware and IT policy control was proposed, (Kruczkowski & Niewiadomska 2014). The study concurred with Renaud, Blignaut, and Venter (2016) study which showed that BYODs like smart-phones not only bring virus into South-African university's computer networks, but are also at risk of being attacked and should therefore be protected using effectively implemented IT security policy. Huber, Flynn and Mansfield (2016) study on IT security policy found that the policy forms an important aspect of proper IT security management. It however argued that difficulties in benefiting from the advantages of IT security policy could be attributed to deviation of IT security policies from the organizational objectives. This view is supported by Olden (2002), which reiterates policy - objective alignment for an efficient and effective information technology security procedures and policies.

In Kenya, a study was conducted by Kimwele *et al.* (2010) on the implementation of IT policies within Kenya's Small and Medium Enterprises (SMEs). It revealed that over 50 percent of the employees were not informed about unacceptable and acceptable use of information systems'

assets of the enterprises. Considering the effects of IT security policies on access control, Nyamongo (2012) noted that there is inconsistent password usage, inadequate user-group management and unsatisfactory implementation of physical access control to information assets within universities in Kenya. Control of user groups is necessary for effective allocation of IT resources as well implementation of authorized of access to the systems. Kiilu, and Nzuki (2014) concurs with the above study and highlights the need for incorporating IT security policy in malware control as a factor to consider when adopting information security management system. On the other hand, Abonyo (2016) argued that, while malware control is good for mitigating and dealing with disasters in library information systems within universities in Kenya, the presence of IT security policy alone without implementable features related to malware control may not be as effective.

The preceding studies reiterate that IT security policy is so important that it should be incorporated in development of information systems security metrics. The studies have also attributed information security breaches to inadequate implementation of IT security policies in the institutions. IT security policy, according to the study, should be aligned to the organizational core objectives. Also, the restrictions imposed by IT policy are seen as necessary to ensure better IT security management. Further highlighted key performance indicator (KPI) for IT security policy to include adoption of the policy, staff sensitization about the policy, establishment of the rules that guide behavior of IT systems' users, specification of penalties imposed on users upon violation of the policies and meeting given industry standards' requirements. While the studies stressed the importance of IT security policy in managing IT security, they however, did not delve into the contribution of IT security policy in quantifying IT security metrics. The sub-elements should therefore, be considered as the building blocks for IT security policy within an organization's IT security structure.

### **2.3.2 Physical Security**

Sandvik (2016) defined information systems' physical security as the protection of information systems: personnel (users), hardware, software, data and networks from physical threats, actions and events, including flood, fire, natural theft, burglary, disasters, vandalism and even terrorism that may cause loss or damage to the information systems. In Uganda, proper physical control

especially barring unauthorized entry into server rooms was found to be a remedy for malware menace (Babu, 2016).

Bichanga and Obara (2014) investigated the challenges facing information systems security management within private universities Kenya, and highlighted computer theft, inadequate physical security, sabotage through cable cuts and system vandalism, among the key challenges affecting information system security management in most Kenyan institutions of higher learning. The study explained that even though physical security practices are overriding other elements of IT security, most universities only consider minimal physical interventions around information asset. However, the few universities which adopt physical security to any levels hardly employ relevant standards as bench-marks for physical security implementation in the universities. The necessity of physical interventions around IT facilities is supported by Mong'ira (2011), which highlighted that the availability of information systems' resources in universities in Kenya is affected not only by hacker activities, but also by physical security incidents like natural disasters, accidental and deliberately actions, including disconnection of network cables, computer theft, vandalism, floods, sabotage, fire, strikes/riots and lighting. The studies pointed many cases where universities' Systems' unavailability has been occasioned by disconnected network cables.

In a research conducted within a private university based in Nairobi - Kenya, Nyamongo (2012) findings concurred with the findings of Bichanga and Obara (2014) on the challenges facing information technology security in the universities. Specifically, it cited poor policies on physical security controls and unfocused IT security frameworks. It claimed that the current IT security implementation frameworks are not comprehensive enough, as they are lacking in contents of physical security. As a result of this, Nyamongo proposed a better IT security management framework which stresses the need for physical barriers around the server rooms as well as signage along critical data lines. While the study recognized physical security as an element of IT security, it however failed to show how the physical security element may contribute to the measurement of the levels of IT security. It therefore suggested the need for a further research to explore the incorporation of IT physical security element in portraying the status of IT security in

a university. The current study, by the researcher has shed light on this area, and the discussions are available in chapter five of this report.

In summary, physical security as an element of IT security involves the protection of information systems against physical threats that may cause loss and damage to information systems. The foregoing studies indicate that loss and damage to information asset occur within universities in Kenya and beyond, yet not all universities take physical security interventions as a matter of priority. Also, in the few universities where physical security is adopted, relevant standards are hardly considered. The studies concur that physical security is so important in IT security that it should constitute a framework for IT security management. Also, they suggest that physical security should form part of IT security metrics, as its level of implementation contributes to the management of IT security. In the present study, which sought to incorporate physical security among other elements of IT security in developing IT security metrics model, is relevant to the suggestion.

### **2.3.3 Network Security**

While studying network security among the US-based universities, Daya (2013) defined computer network security as an IT security approach consisting of the practices and policies adopted to control, prevent and monitor unauthorized access, modification, misuse, or denial of a services in an interconnected computer based resources.

Globally, weak network security has been attributed to breaches of information systems in a member of universities. In the year 2016, for instance, VMware group explored the evolving cyber threat within UK universities and how the institutions can be safeguarded against cyber-attacks. The study revealed that there is a very high likelihood of the universities being attacked due to vulnerabilities in their networks Tzu-Chin (2016). Tzu-Chin showed that 79 percent of the UK universities have experienced damage to reputation due to cyber-attack, whereby 74 percent of those attacked were forced to halt vital research projects due to research data losses associated with cyber related attacks on their computer networks. In 43 percent of the universities, student data; including dissertation materials and exam results have been attacked. Besides, in 25 percent of the universities, critical intellectual property theft had been reported. In

another 28 percent, grant holder research data residing on the computer networks had been attacked. Regarding the attack statistics above, Tzu-Chin argued that the breaches could have been limited if suitable metrics with respect to network security were in place. It concluded that there should be a clear indicator or metrics to help alert the information security conscious community when network and entire information systems security are not adequately addressed.

According to the study by Daya, a stable and secure IT infrastructure confidently supports organizations' core business and also provides safe computing environment. While showing agreement with this, Mullard (2007) further showed that secure computer network increases accessibility of resources to authorized entities, data integrity, data authentication, non-repudiation, confidentiality, privacy and availability. As such, Mullard explained that network security at the elementary levels include network data security, network access control and monitoring, network malware control and network security policy. This view was also held by Broadbent (2007), which argued that security policies around external and internal access control within data networks in Germany could constitute sound strategy for information security management. Peterson and Davie (2007) nonetheless suggested that people, mainly the systems' users should be considered under policy issues. Peterson and Davie also showed that a compromised network security implies that all the resources including data, the host computer, people and all the applications remain vulnerable to security breaches.

Further, Daya (2013) claimed that IT infrastructure supported by insecure network hardly supports organizations' business objectives, since it is vulnerable to attack. In the research, Daya identified increased accessibility of resources to authorized entities, data confidentiality, system authentication, data integrity, non-repudiation, availability and privacy as the most important objectives of secure computer network. Also, Mullard (2007) showed that to ensure network security, there should be regular vulnerability assessment, resource availability, access control, user management, security policy, software patches/updates, malware control, data security controls, and proxy-management. Similar findings emerged in a study by Martins, Eloff, and Park (2001) asserted the need for network hierarchical structure, virtual network segmentations, regular penetration testing, internet bandwidth management tools, alternative internet service

provider, and redundant back-bones in the Local Area Network – LAN, and network security policy as the features of computer network security.

Stressing the role played by computer network in university in South Africa, Jaffer, Ng'ambi, and Czerniewicz (2007) demonstrated that both voice and data communications ride on computer networks, and support workflow through automation tools like ERP in the university. The use of sub-elements of network security in management of information systems' security is further supported by Deloitte Kenya (2011), which conducted a similar study within East Africa. Deloitte, however, suggested the incorporation of people, especially the systems' users, to be considered along the features of network security as mentioned earlier. It showed that network security should be addressed much effectively to ensure safety of the entire information asset. Considering the importance of network security to the entire information systems in universities, Eira and Rodrigues (2009) indicated that even system hackers have to break the network defense first, before accessing the host computer bearing the application systems in order to reach the applications and the data. Eira and Rodrigues thus demonstrated that where there is effective network security, data security could be improved by making the data more difficult to reach by hackers. This view was however, opposed partially by Okibo and Ochiche (2014), which demonstrated that high internet bandwidths in a university computer network has been exploited by system hackers to reach the host computer and finally compromise data security in the host computer.

Makori (2013) studied network security management within universities in Kenya and showed that local computer networks are supplied with high internet bandwidths that facilitate online access to information resources, not only by the stakeholders, but also expose the entire university computer resources to the insecure world through the internet. Makori claimed that the high bandwidth facilitates unauthorized access to the universities' information asset, thus exposing information systems to risk of compromise. This view is supported by Mulwa (2012), which showed that, the sensitive data residing on the Kenyan university networks attracts hackers from both inside and outside the university, who try to access the information and its assets in order to manipulate the information for their selfish gain. Both Mulwa and Makori portrayed network security as a very important aspect of IT security, and separately argued that it

should be considered in an IT security management program. On the contrary, Arora (2010) stressed that despite high internet bandwidths, when effective network security management tools are implemented properly, network layer would still offer protection to data and underlying applications. Arora further showed the need for considering network security as a key element in the entire information technology security that needs to be considered in IT security metrics' formulation.

In summary, network security is viewed as an IT security approach consisting of the practices and policies adopted to control, prevent and monitor unauthorized access and appropriate utilization of resources within interconnected computer systems within a network. While high internet bandwidths provide exploitable opportunities by online hackers, when network security features are implemented effectively, the security extends to the underlying applications, files and data in a host computer. The features of network security should be considered as: hierarchically managed network design; secured network with virtual segmentations e.g. Virtual Local Area Networks - VLANs and user groups; regular penetration testing against network; internet bandwidth management tools; alternative internet service provision, and the existence of redundant back-bones. Levels of implementation of these features can help in estimating IT security status within an organization, but only with respect to network security. It is against this view that network security ought to be considered an element of IT security which remains important in IT security metrics' model.

#### **2.3.4 Data Security**

While analyzing data security the United Arab Emirates, Saleh and Bakry (2008) defined data security as the protective measures that are implemented in an information systems to prevent unauthorized access to computer data, files, databases and websites, thus safeguarding data against corruption, manipulation and loss. This implies that data security, therefore, involves the protective measures that are applied to safeguard the confidentiality, integrity and availability of databases, data resource applications and website of an organization. The study looked at the different information technology risk management methods. It noted that while features that directly address data security play a vital role in information security management, the methods used lack the data security features like encryption. The study claimed that information security

management within universities could be more effective if data security is given high priority in the IT security management program.

In the US, Tomlinson (2016) noted that a hacker broke into computer system of a university in California, and compromised security of data associated with over 80,000 stake-holders - mainly students and faculty members. Tomlinson demonstrated that despite the administrator's knowledge of data encryption requirement in the database, the data security technology was lacking, a situation that was attributed to the vulnerability observed. It concluded, therefore, that there should be a check-list indicating the required data security features in IT security management program, to help remind administrators of the necessary tools and practices as a way of improving data security. The use of checklist of requirements in IT security management program implies the adoption of metrics that would be relied up to show the gaps between the requirements and the levels of implementation achieved. This, in essence, could likely be an expression of the need for IT security metrics based on data security for better management of information security.

The need for data security metrics approach in IT security management was supported by Wei (2014), that analyzed data security situation in US universities based in Dakota and concluded that the use suitable metrics along the lines of databases could help reduce information security breaches within the universities. According to Grama (2014), when approaching graduation time in universities, students want better cumulated average score, and fee clearance, and this interest creates the motivation for attacking university systems. The study agreed that metrics that show the levels to which data security has been implemented in a university's information systems could help limit attempts of attacks.

Ismail and Zainab (2011) conducted an assessment survey on information systems security in Malaysian's special and public libraries with an aim of establishing information technology security status in the libraries. The study considered the principle of least privilege, good backup policies and data recovery procedures to ensure information systems' security. In estimating the status of information technology security, the method used involved identifying the major features of data security in the library information systems, collected data about the

implementation levels of the elements and used average score to portray the IT security status. Analyzing this approach, the metrics approach used in the foregoing study could be inadequate, as it did not consider other major features of data security, like data encryption. Also, the use of simple mean score assumed homogenous weight for all the identified features of data security in contributing towards the metrics. Consequently, a more robust statistical approach that considers commensurate weights for every metrics' element could be more suitable.

In contrast with the study conducted within Malaysian libraries, Casey (2011) suggested that data security consideration should include data encryption at minimum to qualify as a major element of information technology security. On the other hand, Grama (2014) conducted a research to analyze data breaches attributed to institutions of higher education in the United States. Gama found that the number of data security breaches is much more than that recorded. The study considered the adverse effects that the institutions suffer at the height of data integrity breaches and suggested that data security management should include users' restrictions and malware control, besides the features highlighted in the abovementioned studies. Nevertheless, Grama supported the consideration of data security as a key element in IT security management and metrics.

In Tanzania, Luambano and Nawe (2004) pinpointed that student exam management and finance management systems, being web-based, the data therein remains accessible not only through the internet, but also via mobile systems, that makes the university data vulnerable to hackers. Blank (2015) reviewed a case where more than 418 students managed to breach a university's IT security in Uganda and altered their marks to better grades. It argued that using suitable information systems' security monitoring tools could have helped in limiting the breaching of data security. O'Neil (2014) stressed that data security breaches in universities all over the world has increased and as such, there is need for adopting monitoring systems that facilitate proactive security management. Sridhar and Govindarasu (2014) supported this view and showed that data storage, use and transfer through computer networks expose the university's data to cyber-criminals and other threat agents. Also, Sadeghi, Wachsmann and Waidner (2015) agreed with the studies and further showed that hackers associated with students are lured by information

rich networks where they tamper with university's IT systems to adjust grades and fee balances in their favor.

In Kenya, Mulwa (2012) noted increased dependence on information technology by universities in Kenya against heightened information security breaches, and recommended high security control practices to safeguard university data. The study found that in universities in Kenya, students, employees, contractors affect security of information systems. In agreement with this, Deloitte East Africa (2011) revealed that in Kenya, information security breaches have resulted to changes in information systems security management practices, with proactive safeguard measures gradually being adopted. It claimed that the shifts in data security management now focuses on people, especially the users and database managers, who are viewed as the weakest points within the chain of information security system.

Makori (2013) noted that there is increased dependence on information technology within universities in Kenya, where the technology facilitates handling of academic and administrative data at the levels of file generation, storage, processing, caching, long haul transit as well as transfers through local area networks - which in effect expose the university's data to cybercriminals. Apart from user originated data through various applications, Ndung'u (2015) claimed that automation systems like student registration systems, student finance systems and examinations systems are also major sources of data. This concurs with Tarus, Gichoya and Muumbo (2015), which showed that e-learning systems produce so much data in the form of learning modules, examinations and assignments as well as student grades. This implies that so much data is generated in the universities that both routine and proactive measures need to be considered to ensure data security. Proactive security measures could include metrics approach for indicating the levels of implementation of data security features as well as monitoring the performance of the features in automated information systems.

Okuku, Renaud, and Valeriano (2015) concurred with this view, adding that there is need to consider availability of critical servers and applications to ensure data security. The study showed that people are involved extensively in data security management, thus the people constitute elementary points of data security that should be considered to ensure effective

information security management program. In addition, Veseli (2011) justified the need to incorporate not only the people, but also data back-up, malware control and user-groups as effective measures for implementing information systems security in universities. Kimwele, Mwangi and Kimani (2011) stressed those users' restrictions to data resources and systems' back-up should be considered in university IT security management program, by setting up user-groups and alternative places for data recovery in case of disaster, which is in support of position taken by Veseli.

In a synopsis, the foregoing studies stress the importance of data security management control practices along the features of data security in the management of information systems' security. In highlighting the features of data security, they studies concur that sub-elements of data security should include: encryption of data files, users' restrictions to data resources, data backups, data restoration, malware control on systems holding data, hot site, availability of critical servers and applications. Performance levels of the sub-elements should be considered for metrics of data security. Based on data security, the approach taken by Ismail and Zainab (2011) in estimating the status of information technology security within Malaysian university libraries could be lacking. This is because the approach only used average score to portray the IT security status, and assumed homogenous weight for all the sub-elements of data security, implying that a more robust statistical approach that considers commensurate weights for every element could be more suitable in metrics development.

### **2.3.5 Access Control**

According to Shelc (2015), access control is the limitation of entry into an information system only to the authorized persons, using either physical or logical means, as a way of ensuring systems security. Access control is necessary within university's information systems security program to enhance confidentiality, integrity and availability of information resources.

Chan and Mubarak (2012) conducted an explorative study to directly investigate the levels of employee awareness on access control systems within a Higher Education Institution in South Australia. The study showed that the awareness among the employees was generally poor. There was lack of knowledge of information security concepts on physical access control in the

institution, as well as very low levels of awareness on logical access control practices. It however attributed the low level employment of access control facilities to weak policies, especially on IT security. This implies that for the security benefits of the established systems' access control to be realized, there should be strong implementation of IT security policies to make access control more effective.

Human factors must be considered as playing major role in computer hardware availability and general security of all the organizational computer hardware, (Bajaj & Sion 2014). Since the human factors on information security may be deliberate or non-intentional, there are inherent human weaknesses that may lead to serious harm to the organization's information systems. In ensuring better information security, control of access by employee into information systems can be a major tool that if exploited can yield much in overcoming the inherent human weaknesses, (Evyushkin *et al.*, 2014). Eschelbeck and Villa (2003); Audebert and Le Saint (2002); Delimitrou and Kozyrakis (2014), & Ahlgren *et al.* (2012) explained that people who are involved in the systems operations constitute major factors that play significant roles in breaching information systems' security and should be controlled using suitable access control approaches. Bellare, Keelveedhi, and Ristenpart (2013) agreed with this and indicated that people are the weakest point in information security set-up, as they would try to exploit privilege escalation and access unauthorized parts of the network.

Dua, Raja, and Kakadia (2014) debated that since the characteristic behaviour of the systems' users and administrators impacts information systems' security, access into the systems by users should be controlled in user-groups, web content filtration and active directory. It analyzed that well configured active directory and user-group create limiting access boundaries which could improve effectiveness of information systems' security management within universities. However, Delimitrou and Kozyrakis (2014)) argued that some institutions apply user access control guidelines without involving the people from early stages of implementation, which evokes resistance and obstructs information access control technologies' implementation. Delimitrou and Kozyrakis further showed that besides resistance to implementation of access control appliances, access control technologies slow down service delivery by restrictive users' access to production systems.

Colombier and Bossuet (2014) showed that employees' access control should be considered as they are often the weakest link in the protection systems of its information systems' assets, as the damages they cause are related to their levels of disgruntlement. Brickell *et al.* (2011) indicated that information security has been affected by users who share their access passwords contrary to the provided safe computing guidelines, hence exposing the entire information systems to vulnerability. Proper mechanisms need to be presented at every institution in order to identify the most common human factors and also the major associated attacks that threaten computer security.

Kammerman, Monteban and Mud (2000) stressed the need for access control on personal email through an organizations' network, and explained that the access to such emails prompts users to open risky mails, which opens way for spamming, spying and virus injection into the organizational computer network. The study argued that use of portable devices to transfer data from one computer to another could be a dangerous behaviour as it propagates the spread of malware. Fernandes *et al.* (2014) supported the argument and recommended limitation of access by workers to the institutional networks to ensure better IT security management.

In a different perspective, the construct of dissatisfaction among workers at the work - place has been observed to directly relate to major information systems' security breaches in organizations. Therefore, imposing access control on system users can protect the institutions' IT systems in case of staff disgruntlement (Gibson & Van 2000). This includes the disgruntled employees, who out of anger may vandalize the physical information systems for self gratification reasons. Users' disgruntlement could be about dissatisfaction with the organization, superiors, colleagues or situation and should be a factor to be considered in the access control programs. Nevertheless, Gibson and Van further argued that the institutions' information systems could be more harmed, if the disgruntled staff is a senior IT administrator in charge of all systems password allocation and control. Moreover, Gleichauf, Teal and Wiley (2002) identified lack of access control from external networks as among the possible causes for high security risks in information systems. The identification corresponded with Gubbi *et al.* (2013), which showed that inadequate access

control measures for both internal and external networks is a major contributor to information systems' integrity breaches.

In Uganda, studies showed that apart from harmful practices associated with disgruntled staff members on information security, there are other practices which are associated with system administrators, and which also expose information systems to danger. Kancharla and Manapragada (2014) showed that such administrative roles which could create security vulnerability of information systems include lack of regular software patches and updates, uncontrolled access to suspicious hyperlinks, encouraged password loans and encouragement of the use of very weak and easy to guess systems access passwords are major challenges in implementing successful access control. A study by Deloitte East Africa (2011) indicates that insiders present a higher information security threat to east African businesses than outsiders, as the insiders more easily breach the internal access controls. The study showed that information-rich networks found in universities have raised increased appetite for attacks upon university information security infrastructures both from within and outside the organizations, justifying the need for strict access control systems. It argued that insiders are likely to have knowledge of critical data and their locations within the organizations' information network, password for systems access; hence they could gain easy access to unauthorized areas. Also O'Flynn and Chen (2014) concurred with Deloitte, and showed statistical correlation between systems attacks from external sources and the insider activities on information systems.

Ope (2014) studied the IT security situation in universities in Kenya and found that inadequate provision of physical access control was one of the major barriers to information security in the Kenyan public universities. This was attributed, not only to inadequate access control facilities, but also to lack of awareness among IT administrators about the required physical access control and the exact levels of the physical access control that were already installed within the universities. The conclusion made in this case was that the importance of physical security controls around IT systems is given little priority within the universities. The study further concurred with Mulwa (2012), that access control as an IT security element should be composed of: According to the features of access control that constitute its building blocks are: control access from external networks, web content filtration, control of access from internal networks,

well configured active directory and user-group boundaries. While the studies stressed the need for both logical and physical access control for secure IT infrastructure, and the need for increased awareness among IT staff members on physical and logical security access controls, the study did not involve application of access control features towards developing IT security status measurement approach based on access control.

### **2.3.6 Gaps to be Addressed by Objective One**

The studies helped in identifying the IT security elements including IT security policies; physical security; network security; data security and access control in managing IT security. Further, the sub-elements of each element were identified. However, the studies did not include any statistically approached contribution of the IT security elements and the sub-elements in quantifying IT security metrics. Further, Ismail and Zainab (2011) attempts to estimate the status of information technology security within Malaysian university libraries was inadequate considering the method used. Ismail and Zainab's application of average score to portray the IT security status wrongly assumed homogenous weight for all the sub-elements of data security. Every element should have its own coefficient that defines its contribution in building the metrics. These constitute the gap that was investigated in chapter three and found in chapter four, wherein the contribution of the each sub-element towards metrics development was investigated. Therefore a more robust statistical approach that considers commensurate weights for every element should be more suitable in metrics development as conducted in the chapters ahead.

## **2.4 The Relationship Between the Major IT Security Elements' Metrics**

The following section discusses IT security management, the major elements, metrics and their relationships.

### **2.4.1 IT Security Management: Elements and Metrics**

Globally, institutional managers spend much resources in IT security with little information on the net effect of the investment on IT security, O'Flynn and Chen (2014). As supported by

Calder & Watkins (2008), information security management is necessary so as to deal with the ever increasing threats to organizational system's availability, integrity and confidentiality. A review of the IT security practices and activities as centred on the major information technology security elements like network security, data security, personnel, malware control, and security policies, physical security and access control would help in understanding the IT security status within the universities (Lennon, et. al, 2003). Jonsson and Pirzadeh (2011) research on security metrics framework based on operational system attributes showed that no single element can be used to measure the whole information technology security. The study suggested that more relevant elements of IT security should be factored in when developing IT security metrics.

Similarly, Casey (2011) concluded that more suitable IT security metrics models should rely on elements of IT security and not features like the number of attacks and levels of investment in IT security appliances. This implies that an information security manager has to consider beyond the organization's security incident recorded, and the levels of security appliances in the IT infrastructural grid for suitable indicators of IT security status. To measure security status of information technology within the Malaysian libraries, Ismail and Zainab (2011) considered the gap between the security practices and the requirements of international standards, and ranked the practices around IT security elements in a scale based pattern. The approach of measuring security levels on scales based on requirements of international standards is also recommended by Sonnenreich, Albanese and Stout (2006). The technological approach in Malaysia, however, considered only small scope of hardware, networks and software, whose elements were not given elaborate attention.

In Kenya, university-managements have put much investment in IT security appliances towards improving system security, (Bichanga & Obara 2014). Despite continued investment in IT security, there is increased frequency at which security of university information systems are getting breached thus compromising productivity and security of information systems that support teaching, learning, administrative and research activities, (Vacca 2012). The study however, showed that when IT security management is done on the basis of the major elements, and suitable measurement on status considered, management of IT security could be more effective. Makori (2013) suggested that a similar study should be conducted in Kenyan

university set-up, incorporating major elements of information technology security to derive better metrics. In developing IT security metrics, the researcher applied key elements of IT security as well as the international standards, mainly COBIT and ISO 27002.

#### **2.4.2 Information Technology Security Metrics**

According to Tipton and Krause (2000), information security metrics is a distinctive form of measurement that derives its input from data collected on operational levels of elements of IT security, analyzing the data and comparing an entity's state of information security to a predetermined baseline of information security measurements.

The economic environment today is associated with scarcity of resources and calls for suitable metrics to help gauge the performance levels of the elements along which investments are made, Reid *et al.* (2014) & Rayes and Cheung (2007). To ensure prudent utilization of resources and efficiency in any operation, especially within the realms of information and communication technology, a number of institutions of higher education, including universities are feeling the need to prune and reduce computer programs that do not contribute directly to the business needs of the organization, especially those applications and systems that do not clearly and directly support the goals of high priority areas (Neto & Vieira 2010). University investments in information security appliances are as well scrutinized in this perspective of effectiveness due to the scarcity of resources, which include time and money spent against the expected effectiveness (Rostami, Koushanfar & Karri 2014).

Many times, even university system administrators who should be responsible for the function of highlighting the business related value of information security appliances in place do find themselves struggling and unable to demonstrate the strategic value and systems' operational effectiveness against the business value derived therein (Costan, Lebedev & Devadas 2016). This endeavor has remained a significant challenge for the information security professionals over the past many years till now. According to Shostack and Allouch (2001), the key means which should be used to help the information systems' professionals to meet this challenge is the adoption of information technology security metrics based on suitable elements of information

technology security. The elements form the basic operational units for IT security and hence could help constitute a sound metrics approach for IT security.

Overy and Sullivan (2005) showed that information technology security metrics could provide insights on the effectiveness of information security program, show the extents of implementation of information security appliances, levels of information security regulatory compliance, and the departmental practices indicating the ability of all staff members and other stakeholders to adopt information security measures, as well as address security issues for which they are responsible according to their information security policy. In addition, the information technology security metrics could also help in identifying levels of information systems' security risk associated with not taking prescribed mitigation actions and practices within the institution (Chang, Kuo & Ramachandran 2016).

The identification of the security risks provide guidance that helps in prioritizing future resource investments towards bettering information security, (Stallings & Tahiliani 2014). Since metrics provide concrete facts based on functional elements of information technology security and a common methodology for assessing and communicating information systems' risks, they may in addition, be used in raising the level of information security awareness within the organization, (Dworkin 2016). Through the skills gained from experience and familiarity with information systems' metrics, university stakeholders, especially the IT professionals responsible for information security. In addition, Sweet and Yu (2001) concurred that communicating IT security situation to executives of organizations has been a major challenge. It agreed that metrics programs based on elements of IT security could be prepared in a better way to credibly communicate information security situation to the management and other stakeholders.

Alhazmi, Malaiya and Ray (2007) noted that management is mostly concerned about how the information security approach and investments help towards achieving the institutional mission, vision and goals. The executives, however, find it difficult the levels to which investment in IT security achieves this. Breier and Hudec (2011) concurred and indicated that even after investment in information security appliances, the university management would wish to know whether the systems and information resources are more secure after the investment than it was

before the investment. When some appreciable achievements have been made as a result of investment in information systems' security, management and the entire university stakeholders would wish to do a comparison of their information systems' security in relation to systems security of similar institutions in this regard, (Ramsey, Ketts & Buer, 2008). Also, university stakeholders would wish to know whether the entire system is secure enough to safeguard the entire existing information asset (O'Mahony & Timmer 2009). All requirements by the executive regarding performance levels of IT security appliances and controls could be facilitated by the use of suitable IT security metrics model.

All the mentioned concerns of management and university stakeholders provide a guide that defines information technology security metrics with inherent characteristics of effectiveness. This claim is supported by Shah, Novy and Ertl (2007), the inherent metrics characteristics presents tips which can be applied by information systems' professionals to communicate the information security status through metrics to the university management and executives.

### **2.4.3 Source of Data for IT Security Metrics**

An information security metric is seen to be an ongoing process of collection of measurements used to assess information systems' security performance, (Beaubouef, Petry and Arora 1998). Information systems' security metrics models are usually supplied by data derived from operational aspects of information security, to constitute the models' input, Roman, Zhou and Lopez (2013). Some of the data used as the models' input in information security metrics' model come from information system's security's operational activities based on their key elements. The elements in this case include computer network security, data security, physical security, malware control and the general function of information security policies in relation to control over the people, especially the users, administrators and contractors, (Rothermel, Bonn & Marvais 2004). However, data can also come from some other sources including the levels of adherence to policy requirements, (Seegar 2005).

The major function of an information security metric is to help an institution determine whether its security program and appliances already in place are effective and can be relied upon to

improve information systems' security (Stott & Marinho 1979). In doing this, Gamal, Hasan and Hegazy (2011) stressed that the metrics shed light on the value of the security appliances on how they support the institution's core objectives, vision as well as mission. Information systems' metrics can provide insights on effectiveness of the programs, levels of compliance with regulatory requirements on information security, and therefore, informs about the institutions' ability to address security issues.

Sveiby (2001) & Kanstrén, *et al*, (2010) concurred that information security metrics measure the implementation levels of IT security tools, effectiveness, and impact of security program and security appliances in place. To be considered effective, information systems metrics must be meaningful and designed to measure the actions or specifics of the given security program.

#### **2.4.4 Categories of IT Security Metrics**

While several categories of metrics exist, Bartol, Bates, Goertzel and Winograd, (2009) classifies information security metrics into implementation metrics, effectiveness metrics, and impact metrics. Metrics for implementation illustrate the progress and commitment of an institution in putting security controls into place according to the information security policy. An implementation metric may consider requirements by a given regulatory agency, then measuring the percentage of critical information assets for which information systems' risk assessment has been performed against the requirement. The level to which the requirements have been met could be expressed in percentage and the implementation process progresses towards reaching 100% for implementation metrics over time. The target (100 percent) mark is the ideal level of absolute systems' security (Martin 2008).

Effectiveness metrics deals with accuracy and show whether security controls are implemented correctly and meet the intended outcome Dunham, Hartman, Quintans, Morales, and Strazzere (2014). For example, if the purpose for the given information system's security implementation is reducing vulnerabilities, the extent of the reduction of vulnerabilities is the major consideration in this kind of information systems metrics. With this regard, an effective metric majorly reflects

the change in the type, number and severity of critical vulnerabilities detected on servers and information systems as compared to the previous measurements.

Chi, Park, Jung, and Lee (2001) stressed that for information technology security metrics to be effective, the metrics should bear all the characteristics and features of objectivity, and hence they need to be SMART. The study explained that SMART is a contraction for specific, measurable, attainable, realistic /repeatable and time-bound. Therefore, for the information technology security metrics to be truly reliable, the metrics for a given organization should be an indication of how well the security goals and objectives of the organization are being met, and also point to the actions that if taken are likely to improve the organization's overall information systems' security program. Ryan and Ryan (2008) supported that the metrics with clear deliverables, usually meet the outlined criteria and generally considers important factors as: the ease of collecting accurate data that is necessary for a given metric, the guidance to avoid a potential misinterpretation of the given metric, the requirement for periodically reviewing the metrics in consideration and making necessary changes to cope up with the dynamic information systems security arena.

Metrics and measurements in information technology field face a number of challenges. For instance, they view asset value as very easy to measure in general, but difficult to quantify using the common metrics' models. Hougbo and Hounsou, (2015) showed that while threats are common for information systems, it is normally very difficult to measure harm or even the potential for harm, thus forcing most entities to rely majorly on information from external sources as useful for and akin to measurements. Information systems face vulnerability of all kinds depending on the systems security defenses in place. However, the vulnerability of an automated computing device is never easy to quantify (Union, 2014). Therefore the use of modern day security tools provide good information that can be relied upon to gauge the vulnerability levels that a system faces. As reviewed in the foregoing studies, use of data from the lines of operation of IT security as inputs to IT security metrics, could be objective enough in measuring IT security status.

#### **2.4.5 SMART Metrics: Communication of Metrics to Executives**

Chi *et al.* (2001) stressed that for information technology security metrics to be effective, the metrics should bear all the characteristics and features of objectivity, and hence they need to be SMART. The study explained that SMART is a contraction for specific, measurable, attainable, realistic / repeatable and time-bound; and should be compliant to the principle of goal-question metrics (GQM), where goals are derived, relevant questions are asked about the goals and the answers are expressed in metrics format. SMART metrics approach helps to avoid difficulties of communicating about the IT security status with top management. As suggested before, in this literature, metrics should be written in simple language, graphically expressed, especially by incorporating the use of calibrated scales, to enhance understanding and support of the executive.

#### **2.4.6 SMART Aspects of IT Security Metrics**

Breier and Hudec (2011) showed that SMART metrics' setting brings in structured and traceable aspects into the measurability of information systems' security situation. SMART metrics' approach negates possible effects of vague resolutions and conclusions made in regards to the security of information systems supporting business, hence such sound metrics help in creating verifiable trajectories towards the prevailing situation of IT security, with clear milestones as a result of investments in the information' security appliances. Every targets and objectives behind information security metrics' development, can also be made S.M.A.R.T. and as such, brought closer to reality (Dhillon 2007)

In private sector, as analyzed by Kruger and Kearney (2006), SMART goal setting is among the most effective but also least used tools for achieving goals. In many projects as associated with information technology, proper charting of both the projects' outlines and intermediary goals constitutes the initial steps towards developing SMART objectives. Even in general systems' development, installation and maintenance, this approach creates a SMART checklist upon which the SMART objectives can be progressively evaluated. SMART goal setting and approach of work also creates transparency throughout the organization. It clarifies and involves all stakeholders on the way goals came into existence, the importance of the goals, the roles of each

stake-holders and the criteria of the realization and the necessary conformities. Any given goal that one may want to achieve in personal or professional line ought to fit well within SMART criteria through making it conform to the requirements of SMART criteria which are: being specific, measurability, attainability, reality / relevance and timely, (Sajid, Abbas & Saleem 2016); (Skidmore & Rappaport 2002) & Shipley (2000).

Gamal, Hasan and Hegazy (2011) explained that being "**specific**" addresses the exact thing (product) that one wants to achieve, described in much detailed specifications and inherent features to increase the chance of achieving it. It not only handles the concerns about what one wants to achieve, but also the issues of the place / venue of the product, the strategy of achieving the needful thing, including the parties (persons) involved, the resources required, the limitations against the strategy adopted, the need for the product and its possible alternatives. According to Subashini and Kavitha (2011), "measurability" aspect of metrics goals-setting means the identification of exact qualities of what the end product should be. It includes the aspects that will be seen, heard and felt when you reach the specific goal. It majorly involves breaking the given goal down into quantifiable (measurable) elements. Realization of the end product with desired qualities is normally supported by provision of concrete evidence. Neto and Vieira (2010) supported that the need for measurable goals in metrics development goes a long way in refining the real features of the desired product. For example, defining the physical and logical manifestations in the metric's objective makes the metrics' framework clearer, and easier to interpret. In this research the specific and measurability aspects of the metrics is catered for through adoption of specific elements of IT security, and calibrated scale of measurement in a color - coded metric dashboard.

As explained Costan, Lebedev and Devadas (2016), the attainability aspect of S.M.A.R.T. objective concerns the existing conditions / environment resource availability, cultural acceptance and various capabilities that determine the realization of the end product. In assessing whether the goal is attainable, there is need for one to investigate whether the metrics development goal is really acceptable not only to oneself, but also by other stakeholders. Since balancing all the concerned aspects is the key here, there is need to weight the effort, time and other associated costs for the metrics' goal process against other priorities, profits and the

different obligations in the operation. This approach stresses the need for resources like the time, money and talent, which are highly necessary to reach a given goal. The aspect of relevance deals with the justification, giving reasons as to why there is need to reach the given goal metrics set-up, Overy and Sullivan (2005). Therefore, relevance considers the refined objective behind the goal, and assesses whether the approach taken will help realize the set objectives through realization of the goals. Considering the resources used for developing the IT security metrics model in this study, the aspects of attainability and being realistic are achievable.

Seegar (2005) noted that the aspect of time is very important in S.M.A.R.T approach of metrics based goal setting. This involves making a tentative time-based plan of everything that one does, to ensure that the required deadlines are strictly met. Time-bound approaches also involve keeping the timelines which are realistic and flexible across the work-forces to help keep workers' morale high. Seegar indicated that being too stringent even on the time aspect of an organizational goal setting can have the adverse effect of making the entire work environment and staff adopt an unfavourable hellish race against time. Strains at work lead to under performance. With respect to "time" in this study, Chang, Kuo and Ramachandran (2016) & Dworkin (2016) agreed that it is very important to formulate positive metrics that depicts the true picture of the situation as it is at any given time in the organization when setting SMART goals. The metrics' model could be used to provide IT security status instantly over the internet.

#### **2.4.7 Communicating Metrics to the Executives**

Breier and Hudec (2011) identified that another approach applied to appeal to the top management is defining and communicating the current information security situation and the planned state of security in concrete terms. This implies that information system's security managers need to ensure that both the short and the long-term vision for information security, as well as the reason why the vision as conceptualized is important in achieving the objectives and the strategy on how it will be reached, is made very clear. (Bartol *et al.*, 2009). Martin (2008) showed that security managers should use implementation metrics to show work progress on the new and high visibility investment on systems' security initiatives and use the impact metrics for information security to show the institutional value that can be associated with previous

initiatives and the observed impacts that are already in place. This approach appeals to the executives and makes top management prioritize investment in the given ICT security project with respects to the metrics.

Stolfo, Bellovin and Evans (2011) explained that when IT security managers develop the tendency to diligently and transparently report to the executives both / the progress and problems associated with the existing state of affairs and their adverse effects, top management tend to listen and support them. This is because if professional efforts to communicate IT security metrics that executives care about are working, the top management will be much more aware of and be fully engaged in information security strategies and thus support them, (Banerjee, Banerjee, Pandey & Poonia 2016).

Vaarandi and Pihelgas (2014) claimed that when top management have full knowledge of the initiatives and progress made with respect to IT security metrics, the high level awareness helps them to stay informed and also accords them the opportunity to help oversee and fix problems that ICT managers may not take seriously, should they occur. The top management should, therefore, be sent regular security metrics' updates and highlights on any new related concerns of information security when they emerge. According to Seegar (2005), IT security personnel need to understand that in many cases, the university executives easily understand the information expressed in management language, and they need to adopt this approach. Some of effective information security metrics' expressions for executives include the use of percentage to communicate state of the security affairs, for instance, the percentage of information technology budget spent on their information security appliances as compared to peer institutions. Sveiby (2001) concurred with the above that management also keenly listens to any change in percentage of mission-critical information assets in the institution and the complete functions for information security risk assessments that have been achieved since the date when the institution-wide risk management policy / project was issued.

Kanstrén, *et al.* (2010) recommends that information technology managers also need to communicate the change in ratio of information security incidents requiring notification in the institution, especially those that are associated with major breaches. Moreover, Son and Lee

(2011) noted that the total security incidents that have been discovered in institution and how the information security project has helped to minimize the reported information security status within the institution ought to be communicated as well. This should always be supported by the user experience on the information security in the institution.

In summary, information security metrics is a distinctive form of measurement that derives its input from data collected on implementation levels of elements of IT security, analyzing the data and comparing it with the required levels of performance, to help establish the levels of IT security within the organizations. Much of systems security breaches in the universities is attributed to inadequate reliable systems for establishing the security levels prior to the breaches. University system administrators also struggle to demonstrate the strategic value of IT security appliances and their ideal extent of implementation. The need for IT security metrics in portraying the extent of implementation includes the identification of the areas of vulnerability, which in effect provides guidance for prioritizing IT security areas for resource investments, as well as communicating IT security situation to executives.

The relationship between IT security metrics and major elements of IT security is that suitable metrics models are usually supplied by data derived from operational aspects of information security, to constitute the models' input. While there are three main categories of IT security metrics, implementation metrics relates much to this study, which mainly focused on the levels of implementation of the elements of IT security within universities. An implementation metric may consider requirements by a given regulatory agency, then measuring the percentage of critical information assets for which information systems' risk assessment is being performed against the requirement. In universities where IT security metrics have been demonstrated, for example in Australian libraries, the performance levels of the elements of IT security has been expressed either in percentage or in ratios form against the required goals, to facilitate easy communicating of meaning to the executives and general stake-holders. In achieving the goals-originated metrics, the concept of goal-question-metrics (GQM) has been utilized. The above literature also stressed that for information technology security metrics to be suitable, the metrics should bear all the characteristics and features of objectivity, and hence they need to be SMART.

#### **2.4.8 The Gap to be Addressed by Objective two**

The studies reviewed above give insight into the major IT security elements and the benchmarking requirements of IT security standards. In this aspect, the reviews give clear information about their usefulness in information security management within the realms of learning institution, mainly the universities within Kenya, Africa and all over the world. However, the studies did not cover the relationship between information security metrics and the major elements. While the studies converge into an idea that the elements of IT security contribute immensely to IT security management, the knowledge gap is the actual relationship between them. The extent to which each element of IT security affects IT security management and hence the metrics is not clear yet. This presents the need to investigate this relationship. This relationship will be important because from the above studies, it will help in developing IT security metrics model which is grounded on the major elements of IT security as necessary for better IT security management. Consequently, the knowledge gap identified from this review is the quality of relationship between the variable (the elements and the metrics). Investigating this relationship will give the coefficients of every element in relation the metrics; hence will be helpful in developing the model.

#### **2.5 The Existing IT Security Metric's Model**

Axelsson (2000) defined a model as a representation of a systems' structure, typically on a smaller scale, but which is helpful in aiding decision making. Accordingly, the researcher viewed IT security metrics' model as a calibrated systems' graphical representation of IT security metrics as informed by data derived from implementation levels of the key elements of IT security in a university.

Some models have been innovated in the field of electronic communication and information technology to help in gauging IT security performance based on the given set of major operation elements.

### **2.5.1 OCTAVE**

OCTAVE is the acronym for Operationally Critical Threat, Asset and Vulnerability Evaluation; which is a risk-based assessment and planning tool that organizations can use to identify and manage risks in their information security systems. It helps the organization to implement and manage the information systems' security internally through employees who are charged with information security responsibilities. In OCTAVE, risks assessment includes the likelihood of threat agent and vulnerability factors while impact focuses on technical impact and business impact factors at the user operational levels in the organization. Unlike the model in this study, OCTAVE works by focusing on an organization's operational risk instead of the information technology elements themselves and also lacks the implementation levels of the those components. It is insufficient on IT security metrics' premises.

### **2.5.2 Common Vulnerability Scoring System (CVSS)**

The Common Vulnerability Scoring System (CVSS) characterizes vulnerability assessment of information systems, and assigns a numerical score reflecting its severity. The score is ultimately translated into a qualitative representation like critical, high, medium, and low, to help organizations prioritize their vulnerability management processes. This model neither incorporates all the IT security elements, nor does it handle the implementation levels of the elements; hence it is lacking in the perspective of metrics, which is the focus of the current study.

Patriciu, Priescu and Nicolaescu (2006) analyzed the role of security metrics for enterprise information systems in managing IT security, and concluded that information security cannot be easily managed, if it cannot be objectively measured. According to the study, the conclusion is based on the view that metrics is important for assessing the current security status, which in turn forms the reference point for further improvements. It argued that the current approaches for evaluating IT security status are only focused on examining the results of security assessments as means of probing defenses' weaknesses in information security systems, like vulnerability

scanning, penetration testing, without examining the building blocks, as constituted by the major elements of IT security.

Consequently, the study developed an IT security metrics' model that considered only the implementation levels of security policy, security services and their impact on an enterprise's mission. Moreover, the models' weaknesses were that it is based on attack history and the recorded incidents against IT security controls that are already in place. Lack of focus on the major elements of IT security when evaluating IT security status is perceived in the study as not comprehensive enough, considering that security vulnerabilities are identified mainly on the line of major elements of IT security. Therefore, the current study could bring in better metrics as it considered a holistic metrics' approach based on performance levels of the major elements of IT security.

Lin, Ke and Tsai (2015) stressed the need for a systematic approach for measuring security levels of different IT systems in order to obtain evidence of the general IT security levels of different products and organizations. It showed that IT security metrics' approaches based on the major elements of IT security could advance understanding and capabilities in security management within entities. The study showed that major characteristics that ought to be inherent in IT security metrics are that the metrics should be: more quantitative and qualitative, more objective than subjectivity and less static than dynamic in design. In addition to the above, the study characterized a good IT security metrics with: better alignment with organizational goals and objectives to ensure that they are being met; actionable and predictive set-ups; based on a formal and implementable model; execution consistency; dynamism and time-traceability; towards universal acceptance, and using data that's measurable, economical to collect from key operation elements and in consistent with expert judgment. This approach is in agreement with (Creswell & Clark 2017), which in summary stressed that IT security metrics ought to be SMART.

Lin, Ke and Tsai (2015) conducted an empirical study on information systems and came up with an IT security metrics model that was only concerned with intrusion detection system, based on combination of cluster centres and nearest neighbours of intrusion footprints. The metrics approach was based on detecting malicious network traffic through a pattern classifier that promoted correct classifications and connections for effective detection of intrusions and attacks

on information systems. The research proposed a metrics model of a cluster centre and nearest neighbor (CANN) approach, where two distances are measured and summed up for traceability mapping and hence for threat classification. Threat classification levels informed the metrics for information systems' security. The study adopted a statistical Models' approach that was not only analogous to the GQM (goal question metrics) approach, but also applied differential approaches involving mean, and standard deviation on the data collected for the metric's model.

The statistical approach applied in the foregoing study formed rich methodological information for the current study. In addition, it developed an information security metrics that was useful in the perspective of intruder detection patterns. The major challenge of the model was that it was not holistic, as it only covered some aspects of one major element of IT security – the network security, with scarce focus on the sub-elements therein and non inclusion of other major elements of IT security. Moreover, the major pillar of the metrics model, which was cluster centre and nearest neighbour (CANN) was found inadequate, since the presence of long-distant technologies and virtual locations may adversely affect the accuracy of its intruder proximity, and this could make the IT security metrics' approach incredible.

Wang (2005) analyzed information security and developed dual complementary approaches for security assessment. This included analytical modelling coupled with metrics-based assessment. It produced a formal model that permits accurate and scientific analysis of data collected from different IT security processes and not elements, and subjected the data to a collection of mathematical formulas based on goal-question-metrics approach, from which quantitative metrics could be derived. In realization that IT security assessment is inherently complex, Wang showed that the assessment ought to dependent on the assessor's experience and the assessor's resultant description, thus making most aspects of IT security metrics to be qualitative. The study developed an analytical - metrics-based model, facilitated by scientific analysis of data collected from various aspects of IT security implementation, mainly the processes. In the study, the qualitative conclusions were guided by a collection of mathematical formulas analogous to goal-question metric technique. The metrics' model was viewed as a cornerstone for risk analysis and better IT security management. The study proposed the need for a multidimensional assessment of IT security that captures more elements of IT in developing IT security metrics' models.

However, the study was based more on the process for security implementation with little focus on the implementation levels of the major elements of IT security as the basis for the metrics' model. Comparatively, Wang's study agreed with the current study that IT security metrics should have qualitative aspects, which are based on the assessors experience on IT security. Also, it stressed that data collected from the operation of the major elements of IT security should form integral part of the IT security metrics. The current study hence complemented the foregoing study by incorporating the major elements of IT security in the formulation of IT security metrics' model.

Bohme (2010) analyzed the existing scientific approaches for evaluating the returns on information security investments and discussed the relationship between IT security investment models and IT security metrics in California. It showed that cost of IT security should be mapped to the resultant security levels, as supported by the benefits reflected on the levels of implementation of key security features. Bohme proposed a model structure which employed data sourced from the security elements to inform the metrics. Like Wang (2005), Bohme further argued that since the model captured more features related to information security, it should be used for all strategic information security investment decisions as a major element of the overall security budget. Therefore, Bohme's study focused on information security metrics and security investment models which could be useful for balanced investment on organizational IT security. Bohme was concerned about; Return On Security Investment (ROSI) in a business, determining the reasonable levels of information security as well as the right amount of money and time to invest in information security, with an aim of supporting executives' decision making on such investments. The study showed that determining the actual benefits associated with risk-mitigated by a security device is as difficult as measuring the potential risk exposure. As such, it came up with a model for quantifying the returns on information security investment, by establishing the relationship between the IT security metrics and the cost of IT security.

According to Bohme's model, the returns are given by the quotient of; the expected returns less cost of investment, and the cost of investment.

Hence;

ROI =  $\frac{(\text{expected returns} - \text{cost of investment})}{\text{cost of investment}} \dots$  where averages and percentage is used.

However, according to Kitheka (2013), such approaches could not provide reliable IT security metrics upon which improvement could be pivoted. In support of this argument, Jonsson and Pirzadeh (2011) required the application of performance levels of the major elements of IT security towards formulating credible IT security metrics.

While this approach fairly determines the returns on information security investments, according to a study conducted in Nigeria by Nweze (2010), it remains inadequate for determining IT security status in an organization, as the model hardly focuses on the performance levels of the major elements of IT security. Moreover, quantifying the returns on investment (ROI) could be challenging since the expected returns could not always be easily estimated. The current study, therefore, considered data generated from major elements of IT security and their levels of implementation to holistically form the IT security metrics.

Moreover, In South Africa, Safer (2012) showed the need for incorporating major elements of IT security in a systematic way, as organized by a given function in developing an IT security metrics' model. While the framework concentrated more on the security metrics for ICT products, it did not delve much into the key elements driving IT security operations in the organization. The current study therefore captured the inherent characteristics of good IT security metrics and incorporated them alongside the major elements of IT security towards developing the IT metrics model.

Tibenderana and Ogao (2008) considered acceptable use of electronic library within universities in Uganda and focused on metrics' model for measuring the effectiveness of information security awareness program in a pattern similar to the one by Veseli (2011) in Norway. It concentrated majorly on the awareness aspects like knowledge of IT security issues, attitude and behavioural dynamics of information systems' users. While the resultant model was developed on the basis of data collected along the above three aspects of awareness, it could not be applied for measuring information technology security status, as the elements of IT security were not incorporated. Nevertheless, it agreed with the studies in earlier chapters in this research that data collected

from the performance of major elements of IT security should constitute the input for a given metrics' model.

In Kenya, Kitheka (2013) was concerned about the gap between IT security standards' requirements and the actual IT security practices within public universities in Kenya. It noted non-compliance in information security management practices in the public universities in Kenya with regards to the need for implementing effective information security management systems based on measurable levels of IT security. Due to the non-conformity, Kitheka developed a framework for information security management based on internationally recognized IT security guidelines in information security management, to aid management of IT security in the public universities in Kenya. The resultant model for information security management, however, did not include the major elements of IT security as the focal point for establishing performance of IT security. The current study therefore, considered a hybrid of the international IT security standards' requirements and specific deliverables along the line of IT security elements, for the purposes of determining IT security metrics. This approach is supported by Golf (2008) which showed that everything of concern must be measurable to remain manageable; the concept that directly applies to IT security in this study.

### **2.5.3 Summary of the Existing Models and Gaps for Objective Three**

Model by Azuwa, Ahmad, Sahib & Shamsuddin, (2012) called SCADA system designed and hosted in LabVIEW programme. SCADA approach mainly applies to electric power related elements, with little focus on IT security, while the current study focuses on measurement of IT security status based on the performance levels of the elements of IT security. A major shortcoming of Smart SCADA system networks is that, they are connected to external networks, like the internet, thus making the systems vulnerable to threats, especially possible manipulation from entities that may use the network to compromise institutions' power control systems. Patriciu, Priescu and Nicolaescu (2006) model considered only the implementation levels of security policy, security services and their impact on an enterprise's mission. The data collected is based on attack history and the recorded incidents against IT security controls that are already in place.

Lin, Ke and Tsai (2015) model was only concerned with intrusion detection system, based on combination of cluster centres and nearest neighbours (CANN) approach of intrusion footprints. Wang (2005)'s dual complementary approaches for security assessment included analytical modelling coupled with metrics-based assessment. The resultant model was based on data collected from different IT security processes and not the major elements of IT security as the scholastically required basis for the metrics' model. Bohme (2010) model was based on evaluating the returns on information security investments and for security metrics. Ismail and Zainab's (2011) model for university libraries relied on the average score for elements to portray the IT security status was inadequate because it assumed homogenous weight for all the sub-elements of data security. However, every element corresponds to its unique coefficient that shows its contribution in building the metrics.

Tibenderana and Ogao (2008) were based on the effectiveness of information security awareness program. This is similar to a metrics model by Veseli (2011) Moreover, In South Africa, Safer (2012) model was based security metrics for ICT products, it did not delve much into the key elements driving IT security operations in the organization. In Kenya, Kitheka (2013) model was concerned about the gap between IT security standards' requirements and the actual IT security practices within public universities in Kenya.

**2.5.4 Gaps in the Models:**

**$QM = XDS1 + DS2 + DS3 \dots \dots \dots + DSn$**  .....Ismail and Zainab (2011)

- ✓ QM is the IT security metrics, while DS1, DS1.....are the average scores on each data security element. In the above model, only one element of data security is considered. Furthermore, the score has assumed homogeneity in the weight of every sub-element of data security. this is inadequate. The model in this study.
- ✓ SCADA model based on electric power elements, with little focus on IT security.....(Azuwa, Ahmad, Sahib & Shamsuddin, 2012).
- ✓ CANN model was only concerned with intrusion detection system and not IT security elements..... Lin, Ke and Tsai (2015).
- ✓ Tibenderana and Ogao (2008) model was based on the effectiveness of information security awareness program.

- ✓ Safer (2012) model was based security metrics for ICT products and not IT security elements.
- ✓ Kitheka (2013) model was concerned about the gap between IT security standards' requirements and the actual IT security practices.

In summary, the IT security metrics models is use may not reliably measure the prevailing IT security status in most organizations, since the adopted models hardly focus on major elements of IT security. Further they have not incorporated suitable statistical approach that can yield coefficients to uniquely show the contribution of every major element in building the IT security metrics model. More reliable IT security metrics ought to be built on the platform of the implementation levels of the major IT security elements. In building the metrics, data related to the performance levels of the elements should be collected and subjected to statistical functional analysis whose results should be subject to IT security expert's opinion for interpretation. This implies that IT security metrics should be both qualitative and quantitative. The current study, which involved major elements of IT security and applied the GQM approach of metrics' and regression equation in modelling can improve IT security measurement. It is different from the above models since it developed a holistic metrics model composed of the major elements of IT security as;

$Q_M = \beta_0 + \beta_1SP + \beta_2PS + \beta_3NS + \beta_4DS + \beta_5AC + E$  (the error term)..... regression equation model. The details of the equation are explained in the next sections.

## **2.6 THEORETICAL FRAMEWORK**

Here, the researcher reviewed the theory of measurement. According to Sheikhpour and Modiri (2012), measurement is very important in any undertaking, and especially in the field of information technology security. Golf (2008) explained that if you cannot measure everything of concern, then you cannot manage it.

### **2.6.1 The Theory of Measurement**

Measurement theory is one of the branches of applied mathematics that is applicable and vital in quantification of a given phenomenon through data analysis. (Patriciu, Priescu, and Nicolaescu (2006) showed that the main challenge of measurement theory is that measurements of any type

are not the same as the attribute that is being measured. It implies that, if you want to acquire the correct measurement about an attribute, one must consider the nature of the correspondence between the attribute being measured and the measurements that are adopted.

### **2.6.2 Measurement Approach**

Measurement of any given attribute of a situation is a way of assigning numbers of meaning or other meaningful symbols to the situation in a meaningfully predefined way, so that the relationships of the numbers or symbols relate to relationships of the attributes of the features / situation being measured, (Patriciu, Priescu, and Nicolaescu 2006). The predefined way of assigning symbols or numbers of meaning to measure the situation or given attribute is known as a scale of measurement (Gawronski & Payne 2011). The relationships must be empirically verifiable in an accepted way for the measurements to be considered valid.

### **2.6.3 Importance of Measurement Theory**

According to Gawronski and Payne (2011), measurement theory assists us to avoid making meaningless statements, especially those concerning information technology security status. A typical example of such a statement that does not assist in the universities is a meaningless claim, for example, that one university is more advanced in terms of information technology security than another university. While not even an attribute of security being measured is mentioned, the relationship 'more advanced than' applies only to personal opinion of the person making the claim, not any security attribute being measured. However, Kiresuk, Smith and Cardillo (2014) noted that universities have used invalid statements of “improving security of information technology” in the universities, to justify expenditure on IT security infrastructure. This as well, goes against the common management principles that “if system security status is unknown, it is impossible to improve it, (SANS 2007).

As noted by Lingard, Wakefield and Blismas (2013), numbers are usually preferred to symbols in measurement because; they easily portray the relationship between their magnitudes and the intensity of the situations being measured. This means that as the number rises in value, the corresponding attribute being measured is also believed to be increasing accordingly and vise-

vasa. When we measure IT security status in a corresponding number pattern, the resulting numbers are usually, chosen arbitrarily as reasoned out by the experts developing the given metrics' (Gawronski & Payne, 2011). For instance, when we choose to apply a (1 to 5, 1 to 3 or even 1 to 9) rating scale instead of a scale with negative origin, e.g. (-2 to 5), the choice is basically guided by efficiency desired and ease of use by the users of the system in the environments where the problem has been noted. A guiding principle should be that the statistical analysis should yield a corresponding relationship that is meaningful in reality, not just about our whims regarding our perception of the situation, to guarantee that measurement patterns adopted yield statements that are logically meaningful, (Patriciu, Priescu, and Nicolaescu, 2006).

#### **2.6.4 Limitations to Measurement Theory**

De-Vellis (2016) review however, showed that there are limitations to measurement theory. First, measurement theorists attest to the fact that the theory does not provide a complete solution to metrics' problems similar to the one in this research. Measurement theory does not consider random measurement error in its applicability. Secondly, there is no clear distinction between statistical theory and measurement theory; however, the researcher considered this as may be only remotely applicable in this study. To counter this limitation, when the information technology security status' measurement found random errors, an additional method, which considers inclusion of the error term was used as a supplementary and extension method. This limitation was further countered by the additional theories applied in adoption and implementation of ICT systems as shown below.

#### **2.6.5 Theories Applied in Adoption and Implementation of ICT Systems.**

This section discusses the Theory of Planned Behavior (TPB) as well as Theory of Reasoned Action.

#### **2.6.6 A Review of the Theory of Reasoned Action**

The theory of Reasoned Action was developed by Martin Fishbein and Icek Ajzen as an improvement over Information Integration theory (Fishbein & Ajzen, 1975). Reasoned Actions adds the element of behavioral and attitudinal intention in the process of persuasion, in this case for adoption of secure network management practices among technicians in universities. This

theory is comprehensive as it recognizes that there are situations (or factors) that limit the influence of attitude on behavior. Reasoned Action predicts behavioral intention as a compromise between stopping at attitude predictions and actually predicting behavior. Because it separates behavioral intention from behavior, Reasoned Action theory also discusses the factors that limit the influence of attitudes (or behavioral intention) on behavior, and has been applied according to studies, to help adoption of information technology within organizations, (Ajzen, 2011).

This study uses the theory in adoption of general information systems security practices within the universities. First, it achieves change through explaining the advantages of embracing new secure network management approaches. Behavioral intention is concerned with change management in the universities to embrace and cope with new secure network management tools within the information technologies. The theory has been an object of criticism for much of that period and subject to definitional issues about what an attitude is. One of the main recent criticisms is that the theory is not falsifiable (Sniehotta, Pesseau & Araújo-Soares 2014). This means it is impossible to conceive of an argument or observation which could nullify or invalidate them. In contrast, some scholars argue it is falsifiable under reasonable standards.

The theory is important for this study because it has been applied in similar studies for implementation and adoption of information systems in organizations. The persuasion comes in handy to influence users who are the workers in universities as well the network administrators to adopt secure network and general management practices within the universities.

### **2.6.7 Theory of Planned Behaviour (TPB)**

This theory is among the theories for ICT systems' implementation and adoption. According to Armitage and Conner (2001), the theory is among the most influential theories that inform models for information security management in business and organizations. Ajzen (1991) presented the theoretical model - (TPB), which focuses mainly on cognitive self-regulation but takes into account an additional construct of perceived behavioral control. According to Ajzen (1991), perceived behavioral control is the perception of control over the performance and manifestation of a given behaviour. This explains the behavioural patterns of IT systems' users

and administrators together with how the behaviours affect IT security status of the organizations.

Taylor and Todd (1995) studies concur with Mathieson (1991), as they separately analyzed Theory of Planned Behaviour, especially focusing on cognitive self-regulation and taking into account an additional construct of perceived behavioural control. Both researchers concluded that it can influence behaviour of people and predict an individual's intention to use the guidelines of information and communication systems - ICT. This theory applies to the current study as it can be used to focus on cognitive self-regulation and perceived behavioural control to influence the users and information systems administrators in adopting practices that enhance information security within universities in Kenya.

The basis of the theory of planned behaviour is that attitudes together with perceived control and norms, to a great extent, do predict peoples' intentions. The intentions are used to predict deliberate and planned behaviour - which are the practices that enhance information security. According to the theory, intention is determined by three things: attitude, perceived control, and subjective norms. Information security managers can thus work on the three factors to direct intentions of users towards information security practices.

## 2.7 Conceptual Framework

The Major Elements of IT security management

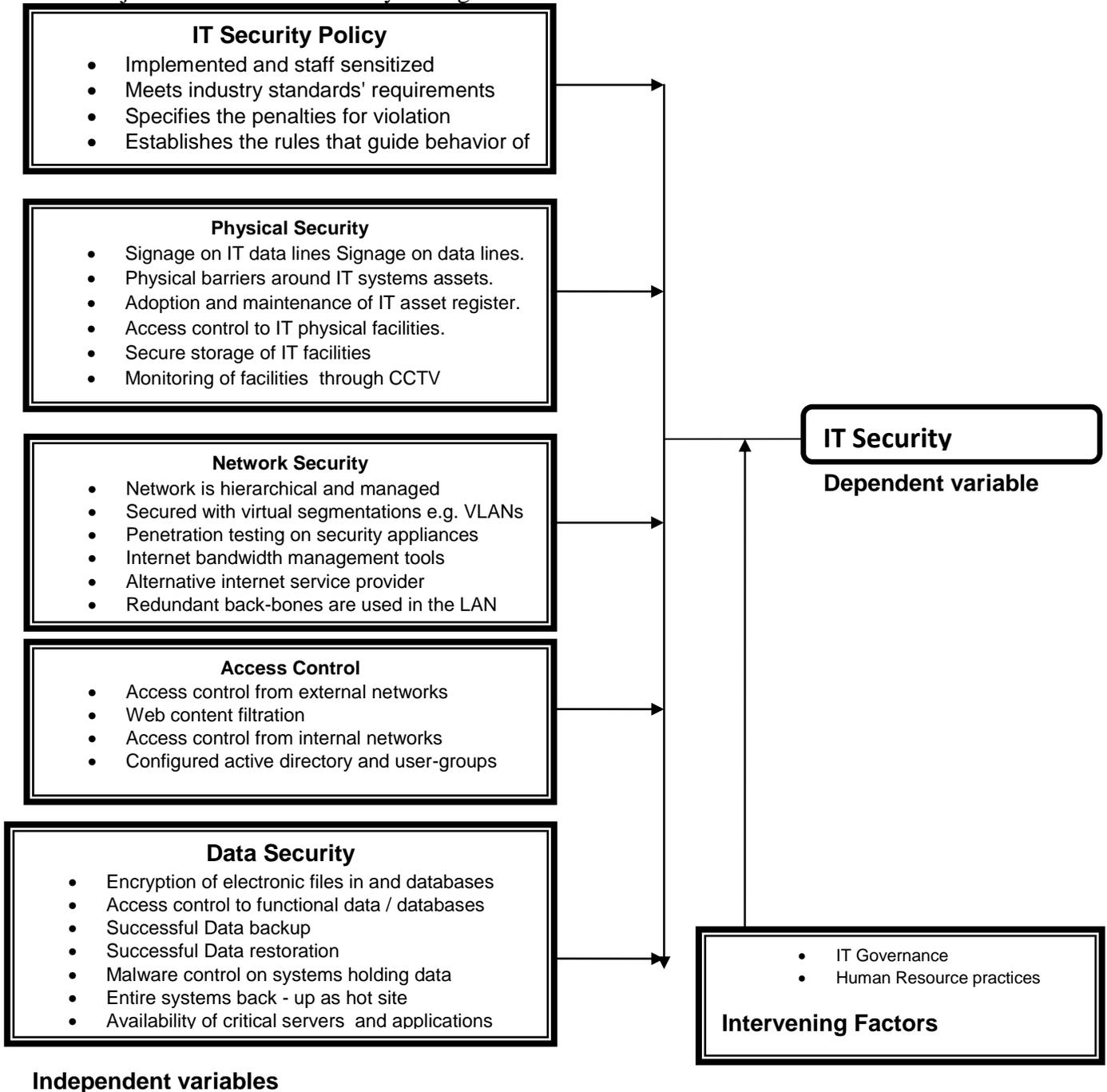


Figure 2.3: The Conceptual Framework

### 2.7.1 Conceptual Framework Explained

This research was conceptualized on the basis of application of the levels of implementation of IT security elements in developing IT security metrics' model. The variables in the conceptual framework map directly into the research objectives as follows: the first objectives' aim was to *investigate the major elements of IT security as per application of the elements in management of IT security within universities in Kenya*. Since the implementation levels of IT security elements are summed up towards developing IT security metrics for the universities in Kenya, incorporating the major elements as the building blocks for security metrics is justified. The left hand side of the conceptual framework indicates the elements of IT security at the top of each box, followed by the sub-elements in a vertical manner underneath, thus illustrating the relationship framework between the elements and IT security metrics.

The second objective, whose aim was to *investigate the relationship between the major IT security elements and IT security metrics in the universities in Kenya*, is also captured in the conceptual framework. The researcher applied the concept of IT security elements' levels of implementation as the constituting blocks for IT security metrics - in determining IT security status in universities in Kenya. This is the reason for linking the IT security elements in the boxes at the left hand side, to the IT Security metrics at the right hand side of the conceptual framework.

For instance, in universities, the major IT security elements include databases security and control of access to data resources within the universities. Data security involves sub-elements like encryption of electronic files in and databases, access control to functional data / databases, successful data backup, successful data restoration, malware control on systems holding data, and availability of critical servers and applications, (Luambano & Nawe, 2004). The study indicated that when information security practices are implemented with respect to the highlighted sub-elements of data security, information systems may be safer. This applies also to all the elements of IT security like security policy, physical security, network security and access control. Furthermore, Arora (2010) indicated that network security elements' practices include network is hierarchical and managed, secured with virtual segmentations, penetration testing on security appliances, internet bandwidth management tools, alternative internet service provider, and redundant back-bones are used in the LAN. Martins, Eloff, and Park (2001) showed that

when all the elements of IT security are applied and managed properly, the entire IT infrastructure enhances general performance and security of information systems within universities.

While implementation levels of the elements of IT security determine the status of IT security, some intervening factor have been identified. Eira and Rodrigues (2009) pointed out that information systems' governance is important in determining the success of the general information systems' security management. Moreover, the study showed that information systems' governance plays a pivotal role not only in networks, but also in the whole information systems' security management. Intervening factors like governance and managements' support remain necessary to facilitate allocation of resources for acquisition of security appliances and development of IT security policies. Human Resource practices have a bearing on the personnel security, as they influence staffing; specify consequences for IT security policy violation, personnel development and discipline.

The last two objectives involved *developing and evaluating an IT security metric's model based on major elements of IT security for universities in Kenya*. The third and the forth objectives were considered in the conceptual framework when the ultimate IT security metrics model, relating IT security elements and the IT security metrics was developed. The relationship is guided by regression model. The ultimate IT security metrics model is coupled with features that enhance visualization, including the dashboard, calibrated metric's scales and informative color coding. The conceptual framework, therefore, involved elements of IT security as independent variables that portray the IT security implementation levels, amidst intervening variables like the IT governance, management support as well as Human Resource practices, which have been put in place within the university.

## **CHAPTER THREE**

### **METHODOLOGY**

#### **3.1 Introduction**

This chapter contains a description of methodology that was used for conducting this study. According to Sarantakos (2012), research methodology is a stepwise and sequential way of providing solution to an already defined research problem. The chapter covers: research design, location of the study, target population, sampling procedure and sample size, sampling procedure, research instruments, pilot study, the validity of the instrument, reliability of the instrument, data collection procedure, data analysis and finally the ethical considerations.

#### **3.2 Research Design**

Matthews and Ross (2014) explained research design as a structured approach of investigation applied to obtain reliable answers to research questions with regards to research problem. It therefore describes the approaches, methods and procedures for parameter reviews, data collection, measurement, as well as data analysis. In this study, the researcher adopted survey method aided by questionnaires as well as interview schedule. According Tracy (2010), survey research design aided by questionnaires helps in gathering data for gaining an insight into underlying relationship between variables, and provides platform for sound quantitative research. Muijs (2010) explained that insight into relationship between variables could be obtained in research through conducting interviews.

##### **3.2.1 Steps in Research Design**

The research was done in three main steps. In step one; the researcher reviewed secondary sources like publications to ascertain the major IT security elements with regards to the requirements of international IT security Standards and in line with the research objectives. Once the elements and their respective sub-elements of IT security were identified, data was collected to investigate their levels of implementation. Therefore, in step two, the researcher developed

questionnaires for collecting data on the opinion of IT administrators and users in sampled universities with regards to IT security elements and metrics. The data was analyzed to generate various coefficients used to formulate an IT security metrics' model, relating the IT security elements to IT security metrics.

Also, metrics' scales corresponding to different implementation levels of IT security was developed with regards to measurement theory's numerical scaling approach, and then mapped on appropriate indicative colour - coding scheme. In step three, the researcher subjected the data collected to regression analysis to give information on the relationship between IT security metrics and implementation levels of each element with regards to IT security standards. This was mapped onto functional form of regression model to give values of coefficients for independent variables. Moreover, a measure of central tendency - the mean was used on the sub-elements to fairly generate metrics values for the major elements.

### **3.2.2 Identifying Information Technology Security Elements in Universities in Kenya**

While the elements were already ascertained in Chapter Two, it helped majorly to address objective one of the research, which was to identify and investigate the major elements of IT security in management of IT security within universities in Kenya. Review of secondary information, especially the research work on information technology security was done to ascertain the key information technology security elements, in chapter two above. The key security elements of information technology are very important, because the levels to which they are implemented, adopted and practiced within the universities can be used to determine the prevailing information technology security status at the elementary levels (Luambano & Nawe, 2004). The major elements include: security policies, physical security, network security, data security, and access control. According to the study, when information security status based on all the key elements are established and combined together, this collectively can be relied upon to portray the information technology security status for the entire information infrastructure in a given university.

### **3.3 Location of the Study**

The study was conducted within the universities in Kenya. The universities are composed of students, lectures administrators and other stake-holders who rely on critical data. For example, academic and financial data remain critical to the universities. Therefore operations of the institutions may halt in the event of data losses and information security compromise. By the year 2018, Kenya had a total of 70 universities; composed of 33 public universities and 37 private universities. They had all adopted information systems to automate their operations.

### **3.4 Target Population**

A target population means a number that represents the whole group of individuals or entities from which the study intends to generalize its research findings (Schindler 2008). According to Kombo and Tromp (2006), population is a group of entities, objects, individuals, or items considered to have certain homogenous attributes, usually represented by a number. Due to the homogeneity, if samples are drawn for measurement, the results are believed to depict characteristics of the entire group. The target population for this research was the number of systems users and administrators of information technology systems in all the 70 universities in Kenya. The accessible population for this study was 910 (13 operation areas x 70 universities = 910). The 13 heads of ICT related departments in all the 70 universities justifiably constituted the population since the actual system users and administrators remain indefinite.

### **3.5 Sampling Procedure and Sample Size**

Sampling means the selection of a representative subset of total individuals within a population of individuals under study, and it is intended to yield some knowledge about the population, Babbie (1998).

#### **3.5.1 Sampling Procedure**

Multiple sampling procedures were applied including: Smith's sampling formula, stratified sampling, ten percent sampling and purposive sampling. Since the users and administrators of

information systems in all the universities in Kenya is not distinct, Smith's formula was applied as:

**Smith's sampling formula**

$$n_0 = \frac{Z^2 \sigma^2}{e^2} \dots\dots\dots\text{Smith}$$

Where:

$n_0$  is the sample size,

$z$  is the abscissa of the normal curve that cuts off an area  $\alpha$  at the tails given by 1.64

$e$  is the desired level of precision given by 0.05

$\sigma$  is the variance of an attribute in the population given by 0.291.

$$n_0 = \frac{1.64^2 \times 0.291^2}{0.05^2} = 91.103 \text{ respondents}$$

Therefore, a sample size of 91 respondents (since there is no fraction of human being) was used.

**Stratified Sampling**

The universities were grouped into two main stata as public and private univesities. This was due to the need for collecting data on IT security elements and IT security measurements from the two main categories of universities in Kenya. As at the year 2018, there were 37 private universities and 33 public universities according to commision for university education, (CUE, 2015)

**Simple Random Sampling**

With regards to the thirteen (13) operation areas identified in chapter two, which are: IT leadership, systems administration, network administration, security administration, database administration, students' finance, students registration, examinations, human resources, internal

audit, library computer , laboratory, and student leadership; and applying ten percent on the 70 universities, ( $13 \times 7 = 91$ ), which is coincidentally equivalent to the Smith's sample size above. Since the universities under each strata were assumed to be homogenous from the perspective of implementation of IT security elements, random sampling was applied to obtain ten percent sample from each strata, and the resultant figures estimated to a whole numbers. For the purposes of this study, ten percent of 70 universities (33 public universities together with 37 private universities, equivalent to sample of 7 universities) were sampled and considered under 13 sections of operation, giving a sample size of 91:  $13 \times 7 = 91$  as shown in the next tables. Team leaders of various categories of information system users and IT administrators formed the target for data collection.

**Table 3.1 : The university Population and the Sample**

University category	Total Number	Sample sizes at ten percent
	<b>Stratified Sampling</b>	<b>Simple-Random Sampling</b>
Public universities	33	3
Private universities	37	4
<b>Total sampled:</b>	<b>70</b>	<b>7</b>

For the public universities, Rongo University, Egerton University and Maseno University were obtained through simple random sampling from a list of public universities in Kenya. Following the same sampling approach, private universities in the sample included University of eastern Africa Baraton, Mount Kenya University, Kabarak University and Kenya Methodist University, which were also sampled randomly.

### **The Purposive Sampling**

Tongco (2007) showed that purposive sampling is a recommended sampling tool for a population where certain groups of individuals may contain more characteristic attributes, and richer in information than other groups within the same entity. Since not every staff member in the entire university work force deals with information systems, there was a need to concentrate on the employees who directly work with university information systems, as this gave reliable data. In this study, users and administrators of IT systems were considered to be richer in

information needed for the study, especially, in IT security experience and data desired by the researcher.

After the representative universities had been sampled through stratified and simple random methods, the researcher employed purposive sampling for the various categories of employees (who interacted daily with IT systems, and were possible victims of IT security breaches ) in each university, to get reliable responses. Pirzadeh (2011) highlighted operation areas in IT administration as basically areas as IT department leadership, network section, database section, IT security, system administration as the major IT operation areas for IT administration. Considering IT systems users, Tarus (2015) noted that students' finance, students' registration, examinations, human resources, internal audit, library, and computer laboratory are the major sections where IT systems are heavily used in the universities in Kenya. In a different study, Ndung'u (2015) study indicated that most staff members in the 13 various operation areas within universities in Kenya have embraced information technology and use it at their places of work.

The current research focused on the highlighted operation areas for data collection. The operation areas were driven by research studies, notably; Pirzadeh (2011), Tarus (2015), Ndung'u (2015), Makori (2013), Mong'ira (2011) & Gichpya and Mumbo (2015), among other studies reviewed in the foregoing chapters. Moreover, data was collected from IT departments from: IT leadership, network administration, systems administration, security administration and database administration. The categories above were preferred for this study for the purpose that employees therein directly interact with information systems in their day-to-day operations within the universities, and were thus potential victims of IT security breaches. Palinkas *et al.* (2015) noted that for information-rich cases in purposive sampling, team leaders of each group can be considered for collection of data, as they are reliable representatives of the entire group. Data was therefore collected from one respondent (the team leader) of each of the thirteen (13) operation areas in every university, including both IT personnel and the information systems' users. Being that a sample of seven (seven universities) was considered for the study, the total sample size was ( $13 \times 7 = 91$  respondents), as shown in the table 3.2 below.

Table 3.2 Purposive Sample sampling

<b>Operation Area (Category)</b>	<b>No of team leader(s)</b>	<b>No of universities</b>	<b>Sample size per category</b>
IT leadership	1	7	7
Systems administration	1	7	7
Network administration	1	7	7
Security administration	1	7	7
DB administration	1	7	7
Students' finance	1	7	7
Students registration	1	7	7
Examinations	1	7	7
Human resources	1	7	7
Internal Audit	1	7	7
Library	1	7	7
Computer Lab	1	7	7
Students Leadership	1	7	7
<b>Totals</b>	<b>13</b>	<b>(13X7)</b>	<b>91</b>

**3.5.2 Sample size:** 91 respondents: 7 universities (4 private, 3 public) and 13 operation areas.

### **3.6 Research Instruments**

Structured questionnaires were adopted in this study as the primary instrument for data collection. In addition, interviews were conducted to collect information from ICT leaders in the various universities. The researcher used two sets of questionnaire which were divided into two sections, with the first part designed to give a brief introduction of the purpose for data collection. The second section was seeking to collect data on the variables adopted for the study. The questionnaires used in this study contained both the closed-ended and open ended questions. The closed ended questions helped collect observations and opinions of the respondents regarding the elements of IT security. The open-ended questions would facilitate freedom of response thus gathering diverse opinion from the respondents as well. According to Graveter and Forzano (2003), questionnaires are recommended for survey because they allow researchers to collect data from a large number of respondents and also provide for an ease of investigation through accumulation of data. In this study, survey was used to collect data on the implementation levels of IT security elements and metrics from the university users and administrators of information systems.

### **3.6.1 Pilot Study**

In order to ensure reliability, especially of data collection instruments, a pilot study was conducted in Kisii University by administering the questionnaires sets and interview schedule. The respondents who were considered in the pilot test were drawn from the target population and the procedures designed to be used for actual data collection were used in the pilot study, as supported by (Muus & Demaray 2005). The university used in pilot test, was not part of the sample for the study. From the pilot study, the researcher would test reliability by administering the same questionnaires and the interview schedules twice to the same people, but at different times. This helped the researcher to detect inconsistencies and ambiguities in the questionnaire, the responses and this would help minimize errors. Typographical errors detected in the pilot study were corrected. It was found that reliability was high. Also, the researcher realized the need to have two separate sets of questionnaire, to help capture relevant information from the two divergent groups of respondents which were: the system users and IT systems administrators.

### **3.6.2 The Validity of the Instrument**

Validity indicates the levels to which the chosen instrument measures the constructs under investigation as it is designed to measure (Mugenda & Mugenda 2003). This study employed expert judgment to enhance face validity and construct validity. Expert judgment is the level of belief that an expert shows in responding to information about a given subject, as based his knowledge and experience. Enhancement of validity by expert judgment improves quality of research, especially during interviews (Gay 2001).

### **3.6.3 Reliability of the Instrument**

To enhance reliability, Test – Re-test method was applied while conducting pilot study for this research. According to Muus and Demaray (2005), Test-Retest method conducts the reliability test on a set of data as measured over time, especially when the same questionnaire is given to the same people twice but at different times and the response are compared. In this study, both

the questionnaires and the interview schedules were administered to the same people at different times (Friday afternoons in week 1 and again in week 2) in one university that was chosen for pilot study. The sets of data collected from week 1 and week 2 were used to calculate Cronbach's alpha ( $\alpha$ ), which is a measure of internal consistency, to help in showing how closely related a set of data were in the pilot study. Cronbach's alpha, which is a coefficient of reliability, was found to be 0.871, thus indicating "good" levels of reliability.

### **3.7 Data Collection Procedure**

Data collection is the process and task of gathering facts and figures from the entities sampled for investigation as necessary for research, (Creswell & Clark 2017). Before gathering data, the researcher applied for and collected research permit from relevant research authorities in Kenya, mainly the NACOSTI, county director of education and county police commissioner. Once the permit was issued, the researcher administered questionnaires to all the 91 respondents from the seven sampled universities. Interview schedule was used to facilitate data collection from ICT leaders in the universities. Three approaches were used to collect data: drop and pick approach where research assistants distributed the questionnaires to respondents, collected them after being filled and returned them to the researcher for data analysis. E-mail communication enabled the respondents to scan and send copies of filled questionnaires for quick data entry. Moreover, interview method was used by the researcher to directly collect information from some respondents, mainly from IT department's leaders.

### **3.8 Data Analysis**

According to Kombo and Tromp (2006), data analysis refers to extracting the facts and figures that have been collected in order to extract information that makes sense about the variables with regards to the population under a given study. The collected data was edited, classified, coded and entered in SPSS software, version 20, so as to facilitate data analysis and presentation in a systematic and clear way. The organized data was then analyzed using statistical tools, in this case SPSS and Microsoft Excel - for presenting summaries. The questionnaire's contents concentrated on the discrete elements of information technology security in universities in

Kenya; hence the analysis yielded the various average values for sub-elements, and the coefficients for the independent elements that constituted the IT security metrics model.

The data collected was analyzed using descriptive statistics measuring central tendency as the frequencies, and summaries presented in form of percentages aided mainly by tables. In addition, regression analyses were applied to show the relationship between pertinent IT security metrics and elements at the implementation levels, as well as to derive values of associated coefficients of major security elements as related in regression model on IT security metrics.

### **3. 8.1 Use of the Average gap Scales for IT Security Metrics**

The primary data on information technology security elements collected through the questionnaire was subjected to descriptive statistics mainly the measures of central tendency – the mean, so as to reveal the average gap under investigation for the sub-elements within the main elements of IT security. The mean value was used as the average security status levels for the given element of information technology under consideration. The average status of security as given by each element of information technology security was categorized into three, depending on the magnitude.

As posited by Ismail and Zainab (2011), both ISO 27001/2 and COBIT standards/ frameworks offer bench-making levels against which the implementation levels of information technology security elements identified above should be mapped, so that the best security practices within the universities can be achieved. For the purpose of this research, the researcher benchmarked on the IT security standards / frameworks requirements of ISO 27001 and COBIT. In this view, security practices short of the standard's requirements defined security gaps within the realms of information technology infrastructure for the universities. The gap analysis between the actual practice and the requirements by IT security standards formed the basis for determining elementary information technology security status. The combined gap analysis for all the elements of information technology security was considered, alongside the corresponding coefficients in the model, as the overall scale of information technology security in the given university.

### 3.8.2 Regression Analysis for IT Security Metrics' Model.

Here, objective two, which was to investigate the relationship between the major IT security elements and IT security metrics used in the universities in Kenya, was addressed. Regression model was recommended for establishing the relationship between dependent variables (IT security elements) and the independent variable (IT security metrics), when used in conjunction with Likert model (Clogg, 1979). Regression equation was therefore applied for the model in order to relate IT security elements and IT security metrics. The researcher adopted regression analysis so as to determine the coefficients of independent variables  $\beta_0$ ,  $\beta_1$ ,  $\beta_2$ ,  $\beta_3$ ,  $\beta_4$ , and  $\beta_5$ , (explained in the metrics model below). Also, it helped determine both the direction and the strength of relationship between the independent variables (IT security elements) and the dependent variable (IT security metrics).

### 3.8.3 The IT Metrics' Model.

The establishment of the model mainly addressed objective three, which was to develop suitable IT security metric's model based on major IT security elements for universities in Kenya. According to Martins, Eloff and Park (2001); Mitnick and Simon (2011) & Luambano and Nawe (2004), the implementation and performance levels of IT security elements are directly related to IT security management. The features of the elements performance levels were used to quantify IT security metrics within universities. The study used descriptive values of central tendencies mainly the mean, as the average performance of the elements as quantified by the implementation levels of the sub-elements. Regression analysis helped for the determination of the relationship between the variables. Respondent's opinions with regards to the elements were quantified using a Likert scale. Regression model was used as:

$$Q_M = \beta_0 + \beta_1 SP + \beta_2 PS + \beta_3 NS + \beta_4 DS + \beta_5 AC + E: \text{Regression equation, Villalonga (2004).}$$

Whereby:

$\beta_1$ ,  $\beta_2$ ,  $\beta_3$  and  $\beta_4$  and  $\beta_5$  are coefficients for the dependent variables while  $\beta_0$  is constant for the model

$Q_M$  = IT security metrics as the dependent unit. In this particular case, the independent variables are: SP = IT Security Policy, PS = Physical Security, NS = Network Security, DS - Data Security and AC=Access Control. Coefficients of the independent variables in the model above were obtained through regression analysis of data in Statistical Package for Social Sciences (SPSS version 20.0).

### 3.8.4 GQM Steps for the IT Security Metrics Model.

The first step involved developing IT security goals and related measurement at the objective's levels. In this research, this included the relative approach to determine the extent to which elements of IT security are implemented in the organization. The second step involved generating questions on the IT security goals to help in defining the goals which prompts answers (data collected) that show the extent of implementation of the IT security elements in the organization. The third step involved computation of average sub-element scores indicating the levels of achievement of the goals. The fourth step involved computation to incorporate averages for performance of the sub-elements of IT security and coefficients for the independent variables as shown below, where the score per item is carried from page to page inform of PHP sessions and tabulated on the bar graph as below.

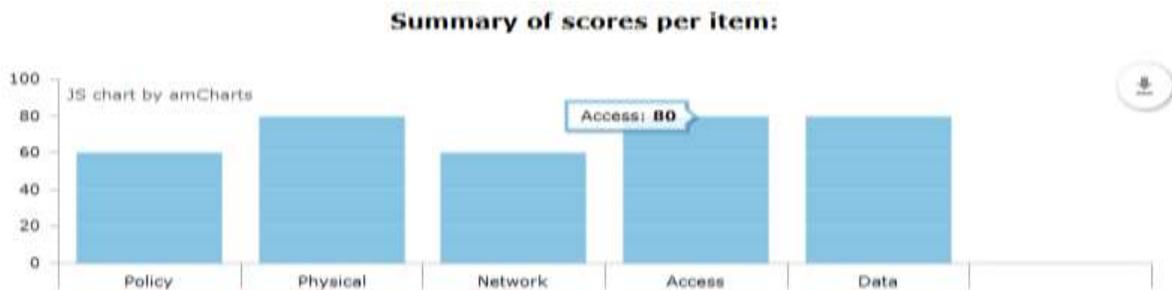


Figure 3.1: sample graph adopted from chapter four

The scores in the above five security elements are then used in the program to calculate the user institution's security score as per the model below,

$$Q_M = 1.9 + 1.6 SP + 0.8 PS + 0.8 NS + 0.8 DS + 0.8 AC \text{ (coefficients obtained from chapter after data analyses)}$$

The fifth step involved further statistical analysis of the data, through the application of regression equation in Likert Model which is conducted using computer program, and then the result become a summarized output of the data analysis. This output constitutes the overall metrics, which is displayed in IT security dashboard, and mapped on the various colour codes for easy interpretation.

### **3.8.5 The IT Security Metrics' Model Implementation and Testing**

Apart from helping to meet objective of establishing the metrics, this section also helped in providing platform for testing the model, according to objective four. Regression analysis helped to show the relationship between the variables through the coefficients. Respondent's opinions with regards to the elements were quantified using a Likert scale. Regression equation was used as:

$Q_M = \beta_0 + \beta_1SP + \beta_2PS + \beta_3NS + \beta_4DS + \beta_5AC$ : Regression equation, whereby  $\beta_1, \beta_2, \beta_3$  and  $\beta_4$  and  $\beta_5$  are coefficients for the dependent variables while  $\beta_0$  is constant for the model.

$Q_M$  = IT security metrics as the dependent unit. In this particular case, the independent variables are: SP = IT Security Policy. PS = Physical Security, NS = Network Security, DS - Data Security and AC=Access Control. Coefficients of the independent variables in the model above were obtained through regression analysis of data in Statistical Package for Social Sciences (SPSS version 20.0).

### **3.8.6 Prototype Development**

The programming languages used were: Hyper Text Markup Language (HTML), Cascading Style Sheets (CSS), JavaScript and Hypertext Preprocessor (PHP). The applications were used on the Chart and graph codes, which were downloaded. For the design, the pages were created to have questions for each of the major element. The system provides buttons options that enable a user to select only one level option for each question. Upon submission, the values for each element of IT security are calculated and an average value is obtained, and then measured in terms of a percentage. For every element, the percentage score is also shown on a graph which is color-coded to help the user know the given elements' security levels. However, contributions of every element to the overall IT security metrics are conducted by the regression model.

### **3.8.7 Program Code for IT Security Model**

*The detailed program codes are available attached in the annex section.*

## **3.9 The Ethical Considerations**

Durkheim (2013) explained ethical behaviour as acting in ways that are consistent with the societal moral principles. The researcher conducted this study with adherence to ethical needs in the study. Firstly, data collection permission was sought and obtained from relevant authorities before collecting any data. All participants, especially respondents, were assured of confidentiality of the data collected from them, stressing that the information they gave would be used exclusively for this academic purpose. Participants would be given copy of the final report summary upon their request.

## **CHAPTER FOUR**

### **DATA ANALYSIS, PRESENTATION AND DISCUSSION**

#### **4.1 Introduction**

This chapter presents: the general and demographic information, the findings addressing objective one, identifying information technology security elements, findings on the levels of implementation of the major elements, findings addressing objective two, the findings addressing objective three, regression analysis for IT security metrics' model, contribution by IT security policy as well as all the other major elements in the model, interpretation of the model, metrics' presentation in color-code, evaluating the IT security metric's model and the IT security metrics' model implementation program.

#### **4.2 General and Demographic Information**

Here the researcher presented at the general and the demographic findings of the study

##### **4.2.1 General Information**

###### **The Response Rate**

A total of 91 questionnaires were distributed to potential respondents, from which a sum of 71 usable questionnaires was returned to the researcher, giving an effective response rate of 78%. The major reasons associated with this high response rate were: i) attached documents of research permit including letter from NACOSTI, county director of education and county commissioner. ii) researchers' introduction letter, as well as the research permission letter from University administration to collect data from the staff members; iii) professional and non ambiguous questionnaire; iv) and the well expressed willingness to maintain confidentiality and to share the final report with the interested respondents. In order to obtain the general and demographic characteristics of the respondents in this study, information was sought on a number of aspects including gender of the respondent, age group of the respondents, category of

personnel, levels of education, years of service in the university, formal and specialized training in IT Security.

#### 4.2.2. Demographic Data

The study found that over 74 percent of the personnel working in the universities as either IT system technicians or users are male, with only less than 26 percent as of the female gender. This could be an indication that information technology field is still dominated much by the male gender, and IT still remains a part of the industry that requires gender mainstreaming in the country.

**Table 4.1: Gender of the Respondents**

<b>Gender</b>	<b>Frequency</b>	<b>Percentage</b>
Male staff	52	74.3
Female staff	18	25.7

**Table 4.2: Institution of the Respondents**

<b>Institution</b>	<b>Frequency</b>	<b>Percentage</b>
Private University	25	35.2
Old public University	24	33.8
New public University	22	31.0

**Table 4.3: Age group of the Respondents**

<b>Age Group</b>	<b>Frequency</b>	<b>Percentage</b>
Staff Under 30 years old	13	18.3
Staff 31-40 years old	47	62.2
Staff 41 - 50 years old	10	14.1
Staff above 50 years old	1	1.4

**Table 4.4: Education Levels of the Respondents**

<b>level of Education</b>	<b>Frequency</b>	<b>Percentage</b>
Staff with Diploma	11	15.5
Staff with Degree	23	32.4
Staff with Postgraduate	37	52.1

<b>Level of Experience</b>	<b>Frequency</b>	<b>Percentage</b>
Staff Below 3 years' experience	12	16.9
3 - 6 years experience	35	49.3
Over 6 years experience	24	33.8
Staff with Any IT security Training	20	29.2
No IT security Training....	50	70.8
Specialized IT Security training	16	61.5
Specialized IT Security training	10	38.5

**Table 4.2: Area of the University**

<b>Operation Area</b>	<b>Frequency</b>	<b>Percentage</b>
ICT staff	28	39.4
Finance	8	11.3
Admissions	5	7.0
Examinations	6	8.5
Human resources	7	9.9
Audit	3	4.2
Library	7	9.9
Health centre	6	8.5
Computer lab	1	1.4
<b>Total</b>	<b>71</b>	<b>100.0</b>

**Category of the University**

In the year 2012, the government of Kenya embarked on a deliberate effort to increase the number of universities. Today, we have not only public and private universities that were in existence prior to the year 2012, but also new public universities and universality colleges that have been chartered by the government. The data collected indicated that majority of team

leaders from IT sections and user departments are aged between 30-40 years old, while 98.3 percent of the leaders are 40 year old and below. This represents a young and energetic workforce which is important for steering ICT systems implementation in the universities in Kenya. Among the respondents, over 52 percent had pursued post-graduate levels of education, 32.4 percent are holders of first degrees while only 15.5 percent had diploma. About 49.3 percent of the section heads had worked for their universities for between three and six years. Over 83 percent of the staff members sampled had worked for the institutions for over three years, with 33 percent having worked in their current universities for over six years. This shows a solid period of staff member' presence in the organization, and is related to the levels of understanding of the ICT systems in the university by the staff members. This shows that the respondents had adequate and reliable information regarding ICT security in their respective universities' information systems.

Formal training in IT security provides IT technicians with sound academic background to enable them understand the current security dynamics in computer system and how to handle them. Table 4.1 above indicates that over 70 percent of the sampled IT staff members have formal training in IT security. Specialized IT security training on the other hand, involves equipping the technicians with knowledge and skills in specific IT security area to enhance their competence. Specialized training handles systems' security under: security audit, network penetration testing, deployment of honey pots, firewalls, among other system specific security matters. The results showed that over 61.5 percent of the IT team leaders sampled had undergone specialized IT security training. This represents competent team to implements IT security appliances adequately within the universities.

In support of the results, establishment of IT security status within an organization, according to Educause Center for Applied Research (2003), would help in prudent and balanced distribution of investment in areas such as personnel training on more security appliances towards mitigating known information security threats and vulnerabilities. According to SANS (2007), training the entire work force is paramount, as long as they interact with information systems, since without knowledge on IT security and status, investment in technology may be haphazard, leading to remote chances of improving information systems' security. Casey (2011) also stressed the

achievement of information technology security mainly through providing training & awareness among all the staff members.

### **4.3 The Findings Addressing Objective one.**

The first objective sought to identify and investigate the major elements in management of IT security within universities in Kenya.

#### **4.3.1 Identifying Information Technology Security Elements**

While the concern about the major elements considered in management of IT security within universities was reviewed in the foregoing chapters, especially in chapter two, it helped majorly to address objective one of the research, which was to investigate the major elements of IT security in management of IT security within universities in Kenya. Review of secondary information, especially the research work on information technology security was done to ascertain the key information technology security elements in chapter two above. The major elements, according to the aforementioned studies, were identified as: security policies, physical security, network security, data security, and access control.

Data was therefore collected from one respondent (the team leader) of each of the thirteen (13) operation areas in every university, including both IT personnel and the information systems' users. The data was analyzed to investigate the levels of implementation of the above major elements of IT security.

#### **4.3.2 Findings on the Levels of Implementation of the Major Elements.**

The study found that the major elements are used across the universities as a guide to managing IT security. It emerged that the major elements as: IT security policy; Physical security; Network security; data security and access control were implemented to varying levels within the universities as shown below.

#### **4.3.3 Element One: Information Technology Security Policy (SP)**

This study revealed that up to 63 percent of the universities have IT security policy in place. However, 37 percent of the respondents indicated that they do not have the policy. This implies that that access and use of information systems' resources are not well guarded in 37 percent of the universities. If up to 37 percent of universities in Kenya have not adopted IT security policy, it is such a substantial level that need to be addressed. This finding, where a substantial number of universities lack IT security policy does not agree with Kimwele *et al.*, (2010), which portrayed security policy as a high level document, usually associated with top management that stipulates the goals and constraints for using IT system, and as such ought to be part of any university.

**Table 4.3: Level of Adoption of IT Security Policy Elements within the Universities**

	V. Ineffective	Ineffective	M. Ineffective	Effective	V. effective
Level of implementation	20	20	28	20	12
consequences for violation	12	28	32	16	12
meets industry requirements	16	36	20	16	12
Guides IT users behavior	20	20	20	12	28

The current study shows that even within the universities where information systems have been adopted and implemented, recognition of IT security policy is not yet fully entrenched. For instance, the results indicated that only accumulation of 32 percent of the respondents agreed that IT security policy is implemented effectively and the staff members sensitized about it. The findings further indicate that up to 40 percent of the respondents do not feel any great impact of the information technology security policy in the universities. The study finding is a departure from the studies reviewed in the literature that portray information technology security policy as a management document, which prohibits users from unsafe computing practices, thus facilitating systems security (Bishop 2003). This implies that computing practices that should be restricted by the use of information technology security policy are hardly controlled within some of the universities in Kenya.

This is further confirmed by the results as summarized in the table, which shows that 60 percent of the respondents felt that the IT security policy in their universities do not effectively guide the behavior of the users of information systems. Fifty two percent of the respondents showed that the policy does not effectively meet the industry requirement, while only 32 percent of the respondents showed that it does. Policies with dispersed conformance from the standards are unreliable and may not offer adequate safeguards and guidelines to information technology security management. This finding is supported by Makori (2013) findings that there are gaps between IT security practices and the industry requirements in universities in Kenya.

From the relevant studies reviewed in the literature above, the information technology security policy informs all users of the requirements for system usage. Information security policy is stressed as the cornerstone for effective information security structure, (Peltier *et al.*, 2005). The policy covers proper risk assessment mechanisms that help in exposing the vulnerabilities to information security and adoption of better security controls, (Hu, Hart, & Cooke 2012).

Further findings showed that among the systems users, the study shows that 47 percent of the users do not know the policy guidelines on sharing system access passwords, while over 51 percent of the users are unaware of any consequences for violating IT security policy. This implies that despite the presence of information technology security policy in some of the universities sampled, violators of the policy do not face any consequence, hence such penalties remain unknown. The current study also indicated that up to 52 percent of the universities have adopted information systems' security policies that hardly meet the industry standards.

Over 64 percent of users are never trained regularly on IT security requirements, while only 42 percent are sensitized on the safe computing practices. Casey, (2011), stresses the achievement of information technology security through implementation of information security policies that involves providing training and sensitization on it. However, over 60 percent of the respondents showed that universities had not implemented IT security policy and sensitized the staff effectively. The inadequate levels of implementing the policy could be attributed to the increasing incidents of systems breach within the universities today. The poor implementation of

information technology security policy is a deviation of the requirement and expectation of the above studies and could adversely affect the organizations information systems' security.

The study further indicated that 72 percent of the respondents confirm that consequences of violating the policy are not effectively spelt out, while only 28 percent of the respondents confirm that the consequences are well spelt out. This generally implies that 72 percent of the university staff across the country is not aware of the IT policy requirements. The finding agrees with a study conducted by Kimwele *et al.* (2010) on the implementation of IT policies within Kenya's (SMEs) and revealed that over 50 percent of the employees were not informed about unacceptable and acceptable practices for information systems'.

#### **4.3.4 The Element Two: Physical Security for Information Systems**

This study found that only 32 percent of the universities implement signage effectively, while 68 percent do not, yet signage along key data lines and computing facilities is very important for ensuring information system security. Forty eight percent of the universities do effectively maintain IT systems asset register, while 52 percent do not maintain it effectively. It was found that 60 percent of the universities do not effectively control access to physical facilities hosting IT systems, while only 40 percent control the physical effectively. The study also found that 76 percent of the respondents agreed that the security of physical computing facilities are not effectively monitored through closed circuit television -CCTV, while only 26 percent of the universities, mainly the private universities do it effectively.

These results concur with Casey (2011), which showed that security levels in the environment surrounding computing facilities ought to be considered in universities. According to Carsey, facilities are kept in some forms of physical enclosures for security provision. These enclosures include behind the grills, perimeter fences and locked server - rooms, (Stallings & Brown 2008). Further, in support of these findings, Mitnick and Simon (2011) considered information systems, and concluded that physical security of computing tools is a crucial element of IT security. Moreover, the study's findings support Mang'ira and Andrew (2014), which highlighted that availability of information systems' resources in Universities in Kenya is affected not only by

hacker activities, but also by physical security incidents like natural disasters, accidental and deliberate actions including: disconnection of network cables, computer theft, vandalism, floods, sabotage, fire, strikes/riots and lighting.

#### 4.3.5 Element Three: Network Security

Anderson (2001) showed that network security helps to safeguard confidentiality, integrity and full-time availability of the computing resources that it supports. This study found that there is high internet bandwidth supply within the universities with more than 60 Percent of the universities subscribing to above 100 Mbps internet bandwidth. Most universities have secondary internet service providers (ISPs) which are 36 percent effective. This finding concurs with Mang’ira and Kitoi (2011) and Makori, (2013), that fast computer networks have made the universities’ data to remain accessible and sharable faster and more widely than before and this exposes the entire university computing resources to the insecure world through the internet.

**Table 4.4: Total Internet Bandwidth Levels in the University**

<b>Internet Bandwidth levels (Mbps)</b>	<b>Percentage</b>
Above 100	60.0
61-100	8.0
30-60	16.0
Below 30	16.0
<b>Total</b>	<b>100.0</b>

While this finding agrees with the two independent studies above, it further shows that most universities have secondary internet suppliers. Some ISPs like KENET allow more than double the amount of internet subscribed in the evenings, throughout the nights and all aver weekends at no additional cost. Due to the high internet supply levels, the universities remain prone to attacks from outside as the external attackers do rely mostly on the fast internet to launch attacks. The study also revealed that all the institutions under survey have adopted firewalls to provide network security at the server levels.

In addition, the study found that 56 percent of the local area networks in the universities are not hierarchical but flat, thus making it difficult to effectively manage them. Fifty two percent of the university networks are still not segmented, meaning users can still access resources freely from any part of the network, without restrictions. For universities with security appliances, 72 percent have not effectively conducted penetration testing, thus are not aware of the effectiveness of the security appliances employed. The study found that 56 percent of the universities do not have effective tools for internet bandwidth management. If the entire internet bandwidth drop in a university's local area network cannot be managed, it could be a sign of misused bandwidth resource.

The current study further revealed that up to 76 percent of the university networks do not have redundant core back-bones. Redundant back-bones help to reach given access networks in case the primary back bone is down, to ensure continuous systems availability. This was suggested as a remedy for system back-up problem by (Ismail & Zainab, 2011). Sixty percent of the universities do not effectively control access from external networks while only 32 percent are controlling the access from internal threats effectively. Sixty percent of the respondents do not effectively implement web-content filtration, meaning access to any universal resource locators (URLs) is not restricted in such universities. This is a security threat as this uncontrolled access may encourage social engineering and spam injection into the university information systems.

The problem of un-managed university network is further shown in the study by the revelation that 56 percent of the universities have not effectively configured the active directories. In some universities, windows server operating systems exist, yet the security features like active directories have never been activated. Over 82 percent of the universities have well controlled user groups with members restricted to given access privileges. Besides, access to given internet sites from the university local area network is restricted in over 75 percent of the universities.

Most of the universities have improper controls for wireless resources like access to the university Wi-Fi, whereby only 44 percent of the users therein use unique user account and a corresponding unique password for every user. Fifty six percent of the universities however,

apply one common and universal pass-word for all and any users within the universities to access the Wi-Fi.

In order to improve security of systems within network infrastructure, various measures are adopted. For instance, the use of IT security training programs, threat awareness program for both system's users and administrators, well configured firewalls, implementation of intruder detection and prevention systems, honey-pots, De-Militarized zones, Unified Threats Management, User-groups, system controlled password expiry, user authentication mechanisms like: bio-Metrics, access control cards and any similar combinations with passwords. The approaches help to minimize security incidents within the high bandwidth internet connection, (Mallard 2007).

**Table 4.5: Availability of Network Security Features**

	<b>Response (percentage)</b>	
	<b>Yes</b>	<b>No</b>
Intruder detection / prevention system	56	44
Honey pots and De-Militarized zones	68	32
Firewall	100	0
Unified Threats Management System	44	56
controlled User-groups	24	76

An intrusion detection and prevention system (IDPS) is a security appliance, which can be a hardware or software that monitors a network for suspicious and malicious activities as well as policy violations, detects the activities and prevents them. The IDPS system then reports any detected violation of policy with to an I.T. Administrator. Bulgurcu, Cavusoglu and Benbasat, (2010) showed that while (IDPS) have been used in most universities across the world to beef up security, some institutions still do not consider them as important remedies for network security. It further showed that user-groups, honey pots and De-Militarized zones are complementary security appliances that enhance network security. The study showed that while 56 percent of the respondents do not use (IDPS), only 44 percent of the respondents apply them. Further, only 32

percent of the institutions sampled use Honey pots and De-Militarized zones in their entire information systems infrastructure.

### **The Application of User Groups in System Security Management**

User groups are very important in information systems' security management as it outlines the boundaries of access to the computer resources, accords different access privileges and also separates systems users from administrators. According to Mohlabeng, Mokwena and Osunmakinde (2012), users-groups are important in the general IT infrastructure security management within South-African institutions of higher learning. Also, Nyamongo (2012) and Jansen, (2010) show that holistic information systems' security framework including user-groups can offer better security management for IT systems in universities.

In this study, it was found that 76 percent of the respondents indicated the availability of user-groups within the universities, results which are consistent with both Nyamongo (2012) and Jansen, (2010) findings. Unified threat management systems (UTM) is a systems' security appliance that handles multiple security features at the same time, for example PRGT, Mikrotik, and Cyberoam systems. They are important in automating security administration for information systems. Also, 56 percent of the respondents confirmed UTM presence in their universities, while 44 percent do not.

#### **4.3.6 Element Four: Data Security**

Data security control practices in a university, for example: encryption, back-ups and restoration are necessary in an organization, (Bulgurcu, Cavusoglu & Benbasat 2010). This research showed that up to 60 percent of the universities successfully back-up their data, while 46 percent retrieve their data effectively after successful back-up. However, only 32 percent of the universities conduct full system back-up while 68 percent of the universities only do simple file back-up.

Data security continues to suffer from malware attack that compromises both data integrity as well as availability. For instance, Eira and Rodrigues (2009) showed that universities' networks are frequent sources of malware. The current study found that 64 percent of the universities do not effectively control malware in their systems. This is because up to 48 percent of the

respondents admit unavailability of critical servers and applications due to malware attack. 49 percent of the users admit that there is no control on transferring data through portable external storage media like flash - disks and memory cards. This finding concurs with Sandvik (2016), that malware spreads fast through such portable devices and this causes multiple losses to information resources, thus rendering information systems unavailable in institutions. The use of external portable storage media contributes so much to malware transfer from one computer system to another, and could be a major concern for data security within universities, Ismail and Zainab (2011). This study found that use of portable devices remains un-controlled within 48.9 percent of the universities in Kenya. The access to the university server room is much restricted in the universities, as 60 percent of the respondents indicated that it is very difficult, as over 90 percent of the respondents showing that it is difficult. Only 47 percent of the universities operate on encrypted files and folders, while 53 percent do not.

The study further found out that academic and financial information were the most valued in the universities in Kenya at 33 percent and 37 percent respectively. Thus, 70 percent of universities attach great value to academic and financial information systems. This supports the Mahnic, Uratnik and Zabkar, (2002) study among the Slovenian universities that showed academic and financial information systems had much high levels of security as compared to other information systems within the university. Ndung'u (2015) and Casey (2011) noted that students and university personnel do compromise mainly academic and financial systems for their selfish interests. It was found that 62 percent of those sampled have lost data within the system, and which they successfully recover.

University has different types of data. Apart from data originated by the user through file generation, automation systems like student registration systems, ERP (enterprise resource planning), student finances and examinations systems are major sources of data, (Ndung'u 2015). According to Selwyn (2007), data classification is very important in determining the most critical data, and prioritizing security appliances' investment approach to apply. The findings in this research showed that 64 percent of the respondents confirmed that there is data classification in their universities, while 76 percent confirmed that they prevent data leak in their systems. The findings agree with Galliers and Leidner (2014) adding that data classification controls access,

reduces data leak , guarantees data integrity and is applicable in most universities and other learning institutions.

Casey (2011) indicated that a server is of central necessity and has become the premier-most target such that access to it may mean compromising the security of the entire information system. Even though the facility is accorded physical security like metallic grills, perimeter fences and locked server - rooms, leaving the system attached to a ready to use accessories may mean easy and quick access into the entire information systems by unauthorized persons, (Stallings & Brown 2008). The study found that 56 percent of the respondents indicated that their critical servers were always attached to ready to use mice and key boards. This poses real risk of quick and easy unauthorized access into the server.

### **Data and System Back-Ups**

Data back-up helps in restoring operations in the event that primary computing data sources cannot be accessed. System back-up considers not only the data back-up, but also the entire application and repositories associated with the data. This is usually more reliable than data back-up since the secondary site acts as a hot site. The study found out that 76 percent of the respondents sampled from the universities conduct regular and automated data and systems back-up, as shown below. This is consistent with findings by Ismail and Zainab, (2011) study on Malaysian's special and public libraries that good backup policies and recovery procedures ensure information system's security.

#### **4.3.7 Element Five: System Access Control**

Shelc, (2015) defines access control as the limitation of entry into an information system to only authorized persons, in order to safeguard confidentiality, integrity and availability of information asset. The Nyamongo (2012) noted that access control to information asset in universities in Kenya is affected by poor password usage and mismanagement of user-groups. Makori (2013) indicates that insiders have breached system access controls for information systems in the universities thus gaining un-permitted access.

This study found that 92 percent of the respondents showed that there is system's controlled password expiry within the universities as shown in below. It also found that bio-metrics and access control cards are rare authentication methods used in the universities to control access into the universities' server rooms. Only 12 percent showed that they use access control cards while 41.7 percent of the respondents indicated the use of bio-metrics to access university server rooms as only 16 percent incorporate the use of access passwords in the authentication.

**Table 4.6 : Access Control Mechanism Applied**

	No	Yes
System controlled password	8	92
Bio-Metrics authentication	58.3	41.7
Access Control Cards authentication	88	12
Mixed / Combinations with passwords authentication	84	16

The study further found out that most universities still rely on physical access control mechanisms like the grills and physical locks to control access into the server rooms. Table 4.7 below shows that only 28 percent of the universities use system based authentication method. Seventy two percent of the respondents still use physical intervention approaches to control access into the server rooms.

**Table 4.7: Nature of Authentication to Access Server Room**

Response	Percentage
System Based	28.0
Physical	72.0
<b>Total</b>	<b>100.0</b>

#### 4.4 Findings Addressing Objective Two and Objective Three

Here, objective two which was to determine the relationship between the major IT security elements' implementation and IT security measurements in the universities in Kenya was addressed by conducting Regression analysis on the relevant data collected. The third objective sought to develop a suitable IT security metric's model for universities in Kenya based on major elements IT security. Regression analysis was applied

##### 4.5.0 Regression Analysis for IT Security Metrics' Model

The researcher adopted regression analysis so as to determine the coefficients of independent variables  $\beta_0$ ,  $\beta_1$ ,  $\beta_2$ ,  $\beta_3$ ,  $\beta_4$ , and  $\beta_5$ , (explained in the metrics model below). Also, it helped determine both the direction and the strength of relationship between the dependent variables (IT security elements) and the independent variable (IT security metrics).

The key security elements of information technology were found to be important for metrics' determination, because the levels to which they are implemented, adopted and practiced within the universities could be used to determine the prevailing information technology security status at the elementary levels, (Luambano & Nawe 2004). The study proved that when information security status based on all the key elements are established and combined together, this will collectively be used to portray the information technology security status for the entire information infrastructure in a given university. These elements were quantified using a Likert scale scores where means / averages were computed for the sub-elements within the main element of information technology security.

Regression model was used as;

$Q_M = \beta_0 + \beta_1 SP + \beta_2 PS + \beta_3 NS + \beta_4 DS + \beta_5 AC$ : Regression model ...as adopted from chapter three for illustration.

Whereby  $\beta_1$ ,  $\beta_2$ ,  $\beta_3$  and  $\beta_4$  and  $\beta_5$  are coefficients for the dependent variables while  $\beta_0$  is constant for the model.

$Q_M$  = Metrics' Q for IT security metrics as the dependent unit.

Independent variables are;

SP = IT Security Policy.

PS = Physical Security,  
 NS = Network Security,  
 DS - Data Security  
 AC=Access Control.

Coefficients of the independent variables in the model above were obtained through regression analysis of data in Statistical Package for Social Sciences (SPSS version 20.0). However, according to Kombo and Tromp (2006), there is a need to add an error term / or factor (E) to such equations.

Thus;  $Q_M = \beta_0 + \beta_1SP + \beta_2PS + \beta_3NS + \beta_4DS + \beta_5AC + E$ , where E is the error term. This is needed to complete multiple regression equation in the model.

**Table 4.13: Regression Analysis**

Model elements	Unstandardized Coefficients		Standardized Coefficients	t	Sig.	VIF
	$\beta$	Std. Error	Beta			
I (Constant)	1.904	0.539		3.533	0.003	
IT security policy	1.620	1.840	0.791	0.880	0.023	1.290
Physical Security	0.800	0.530	0.391	1.509	0.030	1.312
Network Security	0.808	0.879	0.471	0.919	0.035	1.241
Data Security	0.796	0.986	0.398	0.807	0.046	1.485
Access Control	0.788	0.661	0.325	1.192	0.046	1.581
a. Dependent Variable: The IT Security Metrics applied in the University						

Information in the table above was used towards generating the coefficients of IT security elements for completing the equation for metrics' model. The model relates IT security metrics to: IT security policy, Physical Security, Network Security, Data Security and Access Control.

Variance inflation factor (VIF) was used to detect presence of any multi-co linearity among the predictor (independent) variables in the regression analysis. Multi-co linearity occurs when there exists high correlation between predictor's variables (i.e. independent variables) in a model; which can adversely affect precision of regression estimates. The VIF values above show insignificant multi-co linearity among the independent variables. The variables are therefore not highly correlated, and consequently there is no inflation of variance of the regression coefficient, implying that the resultant model is highly likely to give precise estimates for IT security metrics.

Results obtained from the data analysis revealed that there is a positive relationship between IT security metrics and; IT security policy, Physical Security, Network Security, Data Security and Access Control. The associated coefficients' p – values as estimated in the model for all the elements of IT security indicated that there is statistically significant relationship between the elements and IT security metrics. That is, there was high extent to which the result should be considered true in relating the IT security elements to the IT security metrics

Analyses for the constant ( $\beta_0$ ) values for the five variables being (1.904), the p – values were less than 0.05 (i.e.  $p = 0.003 < 0.05$ ). Thus, considering the constant value in the model, the equation became:

$$Q_M = 1.904 + \beta_1 SP + \beta_2 PS + \beta_3 NS + \beta_4 DS + \beta_5 AC + E$$

### **Analysis of the Constant Value ( $\beta_0$ )**

There are both major and non-major elements of IT security in any ICT infrastructure. The non-major elements of IT security including the conscience of personnel security resulting from the sensitization and training, malware control, among other. The minor elements always contribute a small magnitude to IT security situation even in the absence of the major IT security elements. According to the researcher, the constant of 1.904 above represented the combined security role

played by these minor IT security elements. The finding of a value for the constant agrees with Jonsson and Pirzadeh, (2011) about the contribution of the non-major IT security elements.

For IT security policy's estimated model coefficients, the p – values were less than 0.05 (i.e.  $p = 0.023 < 0.05$ ), implying that IT security policy is statistically significant in predicting IT security metrics.  $\beta_1$  value for the security policy being (1.62), the model now progresses to:

$$Q_M = 1.904 + 1.62SP + \beta_2PS + \beta_3NS + \beta_4DS + \beta_5AC + E$$

For physical security, the estimated model coefficients, the p – values were less than 0.05 (i.e.  $p = 0.030 < 0.05$ ) still, implying that physical security is as well statistically significant in predicting IT security metrics at an associated factor of (0.8), thus the equation now becomes:

$$Q_M = 1.904 + 1.62 SP + 0.80 PS + \beta_3NS + \beta_4DS + \beta_5AC + E$$

Completing the model by inserting the factors associated with other elements for IT security, which are ( $\beta_3 = 0.88$ ,  $\beta_4 = 0.796$  and  $\beta_5 = 0.788$ ) for network security, data security and access control respectively, with respective p – values less than 0.05 (i.e.  $p = 0.035$ ,  $0.046$  and  $0.046$ )

Respectively, the final equation becomes;

$$Q_M = 1.904 + 1.62 SP + 0.800 PS + 0.808 NS + 0.796 DS + 0.788 AC$$

### **Interpretation of the Model:**

The coefficients for all the elements of IT security are significant because its p-values are smaller than 0.05. Therefore, for every unit increase in every major IT security element, a significant increase in IT security metrics' value is predicted, holding all other variables constant. As posited by Jonsson and Pirzadeh, (2011) and Simon (2011), the model shows that the constant value could be contributed by other IT security factors that are not considered in this study, as well as all the major elements of IT security in the model.

#### **4.5.1 Contribution by IT Security Policy in the Model**

The coefficient for IT security policy (1.62) is significantly different from 0 because its p-value is 0.023, which is smaller than 0.05. Therefore, for every unit increase in IT security policy, a

1.62 unit increase in IT security metrics is predicted, holding all other variables (IT security elements) constant. The model points to IT security policy as the most important element of IT security. This view is supported by many other research studies. For instance, according to Peltier *et al.* (2005), a well written security policy forms the cornerstone of an effective information security structure. Doherty, Anastasakis and Fulford (2009) showed that a comprehensively written security policy becomes a formal statement comprising of the rules and regulations by which workers, contractors and vendors must abide. Further, the IT security policy being a management document prohibits users from unsafe computing practices thus facilitating systems security, (Bishop, 2003).

Information technology security policy covers proper risk assessment that helps in exposing the vulnerabilities to information security and adoption of better security controls, (Hu, Hart, & Cooke, 2012). Bishop (2003) noted that password implementation, password expiry management as well as privacy controls form key features of information technology security that ensures data confidentiality and integrity. This study and resultant data analyses have found that IT security policy has a metrics factor of 1.62 in the model

$$(1.904 + 1.62 SP + 0.800 PS + 0.808 NS + 0.796 DS + 0.788 AC = Q_M),$$

a value which is much higher than other factors for other IT security elements. This concurs with the above researchers that indeed IT security policy is the cornerstone for IT security management. Without it, the other elements may not be well coordinated to achieve the desired IT security levels within the organization.

#### **4.5.2 Physical Security**

The coefficient for physical security (0.800) is significantly different from 0 because its p-value is 0.03, which is smaller than 0.05. Therefore, for every unit increase in physical security, a 0.800 unit increase in IT security metrics is predicted, holding all other variables (IT security elements) constant. This study found that the coefficient value associated with this element is 0.800. This implies that over 80 percent factor of physical security was found to be contributing to the IT security metrics in the model. Also, in considering the defense in-depth, physical security comes immediately after IT security policy, meaning it is a vital element of information technology. Siponen and Vance (2010) noted that physical access control, which involves

confinement of tangible IT systems within perimeter walls, appropriate signage along network transmission media, secure computing premises are catered for in a well written information security policy. Physical security could highly improve information systems security management in a university set-up, (Jonsson & Pirzadeh, 2011).

Bichanga and Obara (2014) highlighted computer theft, inadequate physical security, sabotage through cable cuts and system vandalism, among the key physical security challenges affecting information system security management in most Kenyan universities of higher learning. The findings also concur with Mong'ira, (2011) which highlighted that the availability of information systems' resources in Universities in Kenya is affected not only by hacker activities, but also by physical security incidents like natural disasters, accidental and deliberately actions, including disconnection of network cables, computer theft, vandalism, floods, sabotage, fire, strikes/riots and lighting. The physical security breaches make universities' Systems' unavailability.

#### **4.5.3 Network Security**

The coefficient for network security (0.808) is significantly different from 0 because its p-value is 0.035, which is smaller than 0.05. Therefore, for every unit increase in network security, a 0.808 unit increase in IT security metrics is predicted, holding all other variables (IT security elements) constant. This study found that the coefficient value associated with this element in then above model is 0.808. This shows that over 80 percent factor of network security contributes to the IT security metrics in the model. Also, in considering the defense in-depth, network security comes in third layer after IT security policy. This implies that network security is a vital element of information technology. The findings agree with the above studies as well as the suggestion by Ismail and Zainab (2011), that network security elements should be used towards developing sound IT security metrics. Also, the findings concurs with Arora (2010) that stresses the need for considering network security as a key element of the entire information technology security.

Makori (2013), studied the network security for universities in Kenya and showed that local computer networks are supplied with high internet bandwidths that facilitate online access to information resources not only by the stakeholders, but which also expose the entire university

computing resources to the insecure world through the internet. According to Daya (2013), a stable and secure IT infrastructure confidently supports organizations' core business and also provides safe computing environment. A compromised network security implies that all the resources including data, the host computer and all the applications remain vulnerable to security breaches, (Peterson & Davie, 2007).

#### **4.5.4 Data Security**

The coefficient for data security (0.796) is significantly different from 0 because its p-value is 0.046, which is smaller than 0.05. Therefore, for every unit increase in data security, a 0.796 unit increase in IT security metrics is predicted, holding all other variables (IT security elements) constant.

This study found that the coefficient value associated with this element in the above model is 0.796. This shows that 79.6 percent factor of data security contributes to the IT security metrics in the model. Also, in considering the defense in-depth, data security comes in the central part of the circular layer, meaning all the above layers are designed to protect data. This implies that data security is a very important element of information technology. The findings agree with the above studies as well as Lennon, et. al, (2003) that data security helps in understanding the IT security status within the universities.

Grama (2014), conducted a research to analyze data breaches attributed to institutions of higher education in the United States and indicated that the number of data security breaches is much higher and adversely affects information system security. As such, Casey (2011) suggests that data security should be a key element of information technology security. Data security controls like encryption, back-ups and retrieval are so important, that they are usually incorporated in the security policy, (Bulgurcu, Cavusoglu, & Benbasat, 2010). While data security contributes this much to IT security metrics, this study that data security implementation levels are still weak, as most files and databases are not encrypted within the universities.

#### **4.5.5 Access Control**

The coefficient for access control (0.788) is significantly different from 0 because its p-value is 0.046, which is smaller than 0.05. Therefore, for every unit increase in access control, a 0.788 unit increase in IT security metrics is predicted, holding all other variables (IT security elements) constant. This study found that the coefficient value associated with this element in the above model is 0.788. This shows that 78.8 percent factor of access control contributes to the IT security metrics in the model. Also, in considering the defense in-depth, the layered approach is the central access control philosophy, which stresses that if security is provided in a layered fashion, with each layer having its unique security provisions / barriers to systems' entry, data will remain safe. The philosophy of the layered approach to security provision in defense - in - depth is that all the above layers are designed to protect the lower layers, as one has to overcome the barrier in the current layer before accessing the lower one. This implies that system access control is a very important element of information technology.

This finding concurs with Shelc (2015) which defined access control as the limitation of entry into an information system to only the authorized persons, in order to safeguard the confidentiality, integrity and availability. Makori (2013) indicate that insiders have breached system access controls for information systems in the universities thus gaining unpermitted access. The findings agree with the above studies as well as with Siponen and Vance (2010) which notes that systems access control must be catered for in a well written information security policy to ensure proper information systems security management. However, levels of access control implementation are found to be inadequate in most of the universities.

#### **4.6 The Unique Ratio Coefficient**

A unique model coefficient ratio of (2: 1) was found in this study. The researcher reviewed the metrics' model above and noted that when the coefficient factors are rounded off to one decimal place, the equation becomes;

$$Q_M = 1.9 + 1.6 SP + 0.8 PS + 0.8 NS + 0.8 DS + 0.8 AC$$

Thus:

$$Q_M = 1.9 + 0.8 ( 2 SP + PS + NS + DS + AC )$$

This implies that among the major IT security elements, the IT security policy weighs twice as any other major element in the model.

The fitted model was diagnosed and found to be statistically significant at 5 % significant level (regression p – value < 0.05). This shows that IT security metrics is positively determined by a combination of IT security policy, physical security, network security, data security and access control. The adjusted R – Square value is an indicator of how well the model fits the data, hence showing the strength of a model in forecasting.

#### **4.6.1 Scaling of the IT Security Metrics**

Research studies emphasize measurement as an important tool for IT security management. For instance, Golf (2008) explains that for everything of concern, if you cannot measure it, then you cannot manage it. While SANS(2007) stresses that if system security status is unknown, it is impossible to improve it. Further, according to Sheikhpour and Modiri (2012), measurement is very important in any undertaking, and especially in the field of information technology security.

#### **4.6.2 Measurement Approach**

Benneworth (2015) found that everything can be measured with certainty. The study stressed that for the measurement to be comprehensive, one should be limited to a few key areas at a time and getting a methodical plan that's more likely to yield required measurements of state. With respect to Benneworth, (2015), this study for determining IT security metrics model, is confined to contributions of the five major IT security elements towards the metrics. From the background of measurement theory, measurement of any given attribute of a situation is a way of assigning numbers or symbols of meaning to the situation in a meaningfully predefined way so that the numbers or symbols relate the attributes / situation being measured, (Patriciu, Priescu, and Nicolaescu, 2006). The predefined way of assigning symbols or numbers of meaning to measure the situation or given attribute is known as a scale of measurement (Gawronski & Payne 2011).

Further, according to Lingard, Wakefield and Blismas (2013), numbers are usually preferred to symbols in measurement because they easily portray the relationship between their magnitudes and the intensity of the situations being measured. This means that as the number rises in value, the corresponding attribute being measured is also believed to be increasing accordingly and vice-versa. A guiding principle should be that the statistical analysis should yield a corresponding relationship that is meaningful in reality, not just about our whims regarding our perception of the situation to guarantee that measurement patterns adopted yield statements that are logically meaningful, (Patriciu, Priescu, and Nicolaescu, 2006).

When measuring IT security status in a corresponding number pattern, the the numerical guide is usually chosen as reasoned out by the experts developing the given metrics' matrix, as the choice is basically guided by efficiency desired and ease of use by the users of the system in the environments where the problem has been noted (Bond & Fox 2015). With regards to Gawronski and Payne (2011), Lingard, Wakefield and Blismas (2013), Patriciu, Priescu, and Nicolaescu (2006) & (Bond & Fox 2015), the resercher considerd that the numerical strenth of the sub-elements constituting the major elements of IT security should sum up to unity for each of the five major elements of IT security. Scores for perfromance of each sub-element within the major element would be determined by the extent to which the requirements of a given IT security standard in use is met, (Lodgaard & Ashland, 2011). Therefore the metrics highest (maximum ) and lowest (minimum) values in the model would be;

From the model:  $Q_M = 1.9 + 1.6 SP + 0.8 PS + 0.8 NS + 0.8 DS + 0.8 AC$

OR factorized: as

$$Q_M = 1.9 + 0.8 (2 SP + PS + NS + DS + AC) + E$$

The maximum metric's value equals 6.7, approximated metrically to 7.0, while the lowest metrics' value equals 1.9, approximated metrically to 2.0, as guided by (Bond & Fox , 2015). According to Gawronski and Payne (2011), the predefined way of assigning symbols or numbers of meaning to measure the situation or given attribute is known as a scaling measurement. The scale for IT security metrics according to this study would be ranging from 2.0 to 7.0.

#### **4.6.3: Deriving the Values for the Minimum and the Maximamun Values**

**Minimum value:** Suppose all the elements of IT security are each zero,

The equation

$$Q_M = 1.9 + 0.8 (2 SP + PS + NS + DS + AC)$$

becomes  $1.9 + 0 = \mathbf{1.9}$ .

**Maximum Value:** Suppose all the elements of IT security are each full to unitary value,

The equation

$$Q_M = 1.9 + 0.8 (2 SP + PS + NS + DS + AC) \text{ becomes}$$

$$1.9 + 0.8 (2+1+1+1+1) = 1.9 + 4.8 = \mathbf{6.7}$$

Hence the metrics here and takes values from 6.1 - 7.0 as approximations;

#### 4.6.4 Metrics' Presentation in Color-Code

According to Trethowen, Anslow, and Welch (2015), the measurements' outputs should be related to colour codes for better visualization, an idea that is further supported by Kruger and Kearney (2006). The measurement from the above metric's model were categorized into three, depending on the levels of implementation of the IT security elements, and then mapped into corresponding colour codes associated with the different security status as shown below.

Red colour was used to imply severe security status that needs immediate attention. In the model implementation, it takes measurement values from 2.0 - 4.0. Yellow means insecure environment that needs consideration for improvement and takes values from 4.1 - 6.0, while Green means a safe computing environment that needs to be maintained and takes values from 6.1 - 7.0 as shown below. This now completes the presentation in chapter three since the minimum and maximum values have been determined.

**Table 4.14: Metrics' Presentation in Color-Code**

1.9	3.1	4.1	5.1	6.1	6.7
Severe security status <i>(Needs immediate attention)</i>		Insecure <i>(needs improvement)</i>		Safe <i>(Needs maintenance)</i>	

## **Findings Addressing Objective Four**

The fourth objective sought to determine the applicability of the developed IT security metrics' model for universities in Kenya.

### **4.7 Evaluation the Applicability of the IT Security Metrics' Model**

The study handled the evaluation and validation of the developed IT security metrics' model as follows;

#### **4.7.0 Evaluating the IT Security Metric's Model**

##### **4.7.1 GQM Steps for the Model**

The first step involves developing IT security goals and related measurement at the objective's levels, which in this research, included the relative approach to determine the extent to which elements of IT security are implemented in the organization. The second step involved generating answers, through data collection and analysis, which show the extent of implementation of the IT security elements in the organization. The third step involved specification of measures in form of ratios or percentages indicating the levels of achievement of the goals in relation to the expected performance (implementation levels). The fourth step involved analyzing and validation of the data on the performance of the elements of IT security in the organization. The fifth step involves statistical analysis of the data, through the application of regression equation in Likert model which is conducted using computer codes, and then the result constitutes the overall metrics, which is displayed in IT security metrics' dashboard, and mapped on the various colour codes for easy interpretation. The implementation of the IT security metrics dashboard helped to achieve the validation need for the model.

##### **4.7.3 The IT Security Metrics' Model Implementation**

IT security metrics is conducted according to the model:

$$Q_M = 1.9 + 1.6 SP + 0.8 PS + 0.8 NS + 0.8 DS + 0.8 AC,$$

This summarizes into:

$Q_M = 1.9 + 0.8 (2 SP + PS + NS + DS + AC)$ . The program form implementing it is attached at the appendices section.

This implies that the maximum metric's value equals 6.7, approximated metrically to 7.0, while the lowest metrics' value equals 1.9, approximated metrically to 2.0. In measurements, there should be the minimum and the maximum values as guided by (Bond & Fox 2015). The scale for IT security metrics according to this study would be ranging from 2.0 to 7.0.

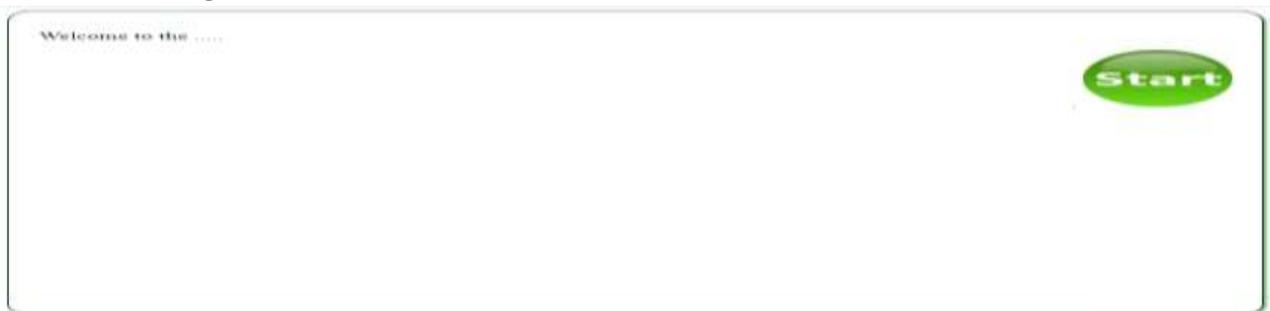
#### 4.7.4 Applicability of the IT Security Metrics' Model

The model was (and is up to now) hosted on a local server at Rongo university server – room. The server is configured with a public IP address to facilitate international access through the internet via (<http://41.89.203.228/oguk>). The link leads to the online IT security metrics dashboard.

##### **The Online IT Security Metrics Model Dashboard (Real Life Application)**

When one clicks (<http://41.89.203.228/oguk>), the dash board appears as shown below, when one clicks on the “start button”

**Table 4.15: Starting Point**



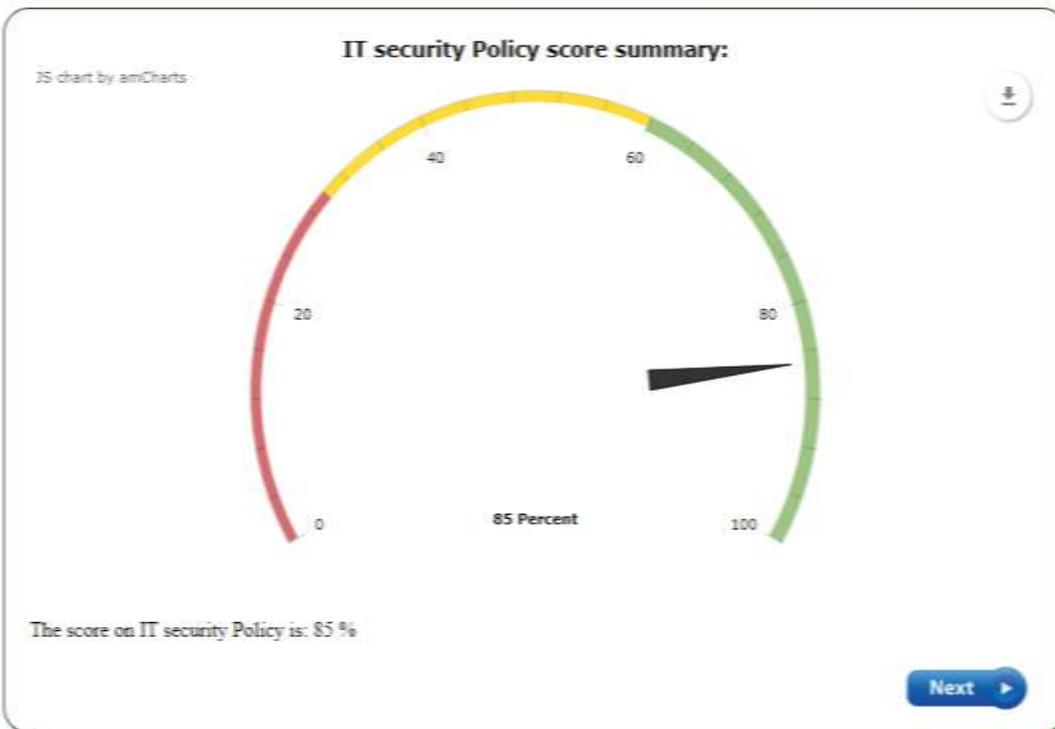
**Table 4.16 : IT Security Policy Measurement**

*Scale based rating for the performance levels of IT Security Elements*

For the tables below, please rate your response in a scale of 1 – 5, where, 1 = (Very ineffective), 2 = Ineffective), 3 = (Moderately Effective), 4 = (Effective), 5 = (Very Effective). You are requested to indicate the performance levels of IT security based on the elements below.

<i>Element one:</i>	<i>IT security Policy</i>	<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>
<i>1</i>	<i>What is the extent to which the policy is implemented and staff sensitized about it in the university?</i>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
<i>2</i>	<i>Meets the industry standards' requirements?</i>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
<i>3</i>	<i>Specifies the penalties for violation?</i>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
<i>4</i>	<i>Establishes the rules that guide behavior of users</i>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

The dashboard loads after clicking the “submit button”



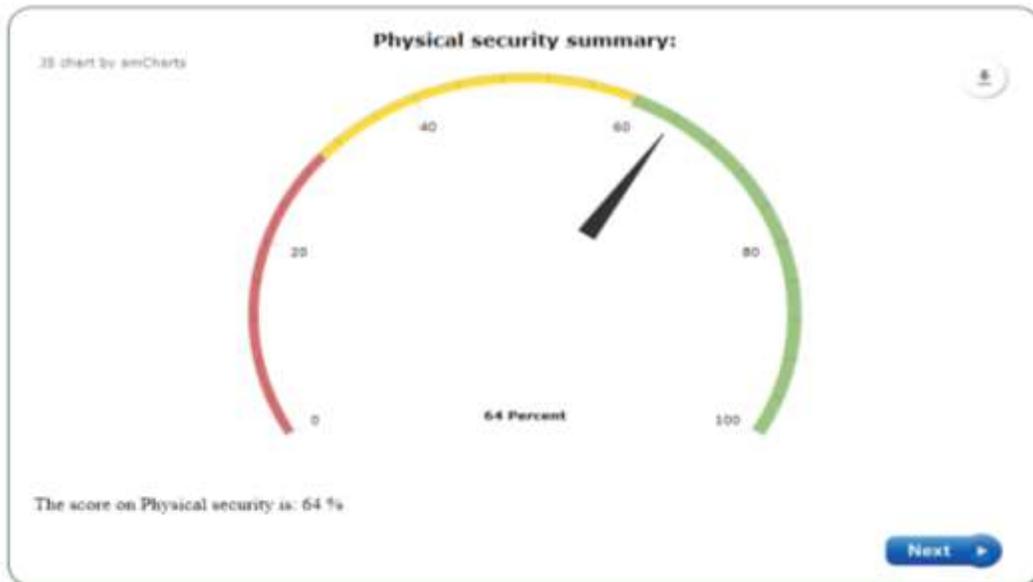
**Table 4.17: Physical Security Measurement**

*Scale based rating for the performance levels of IT Security Elements*

For the tables below, please rate your response in a scale of 1 – 5, where, 1 = (Very ineffective), 2 = Ineffective), 3 = (Moderately Effective), 4 = (Effective), 5 = (Very Effective). You are requested to indicate the performance levels of IT security based on the elements below.

<i>Element two:</i>	<i>Physical security</i>					
What is the extent of:		1	2	3	4	5
1	implementation of Signage / mark posts on IT data lines?	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
2	implementations of physical barriers around IT systems assets?	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
3	implementation, adoption and maintenance of IT asset register?	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4	access control to physical facilities hosting IT systems?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
5	secure storage and monitoring of facilities e.g. through CCTV?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

The dashboards the loads.....



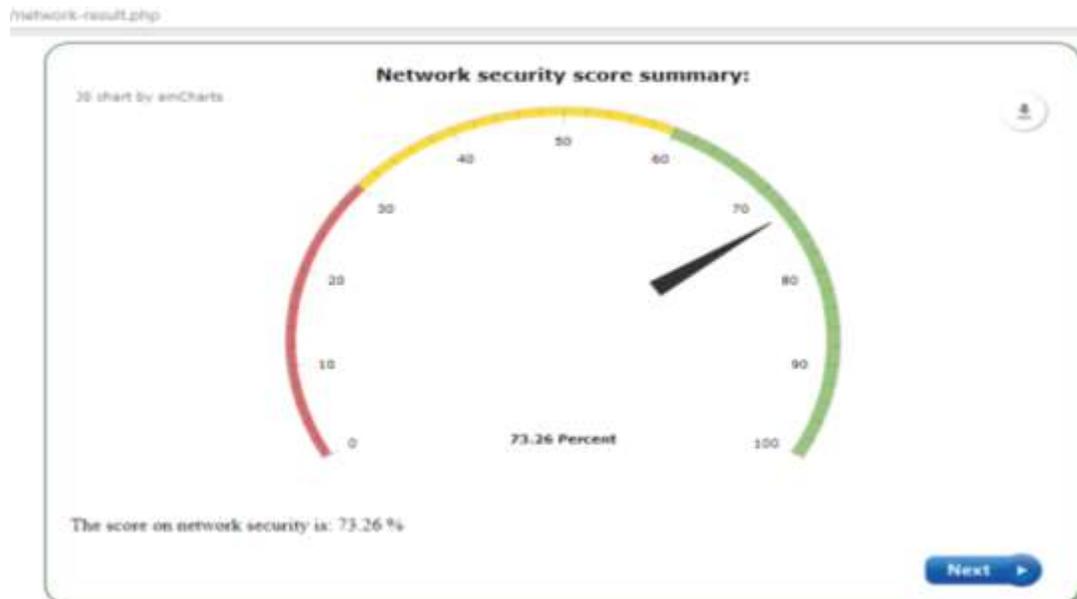
**Table 4.18: Network Security Measurement**

*Scale based rating for the performance levels of IT Security Elements*

For the tables below, please rate your response in a scale of 1 – 5, where, 1 = (Very ineffective), 2 = Ineffective), 3 = (Moderately Effective), 4 = (Effective), 5 = (Very Effective). You are requested to indicate the performance levels of IT security based on the elements below.

<i><b>Element three:</b></i>	<i><b>Network Security</b></i>	<i><b>1</b></i>	<i><b>2</b></i>	<i><b>3</b></i>	<i><b>4</b></i>	<i><b>5</b></i>
<i>1</i>	<i>What is the level to which:</i>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
<i>2</i>	<i>your computer network is hierarchical and managed?</i>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
<i>3</i>	<i>your network is secured with virtual segmentations e.g VLANs?</i>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
<i>4</i>	<i>you conduct penetration testing against network security appliances?</i>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
<i>5</i>	<i>you have internet bandwidth management tools?</i>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
<i>6</i>	<i>there is alternative internet service provider (ISP) is used?</i>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
	<i>redundant back-bones are used in the LAN?</i>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

The dashboard loads...



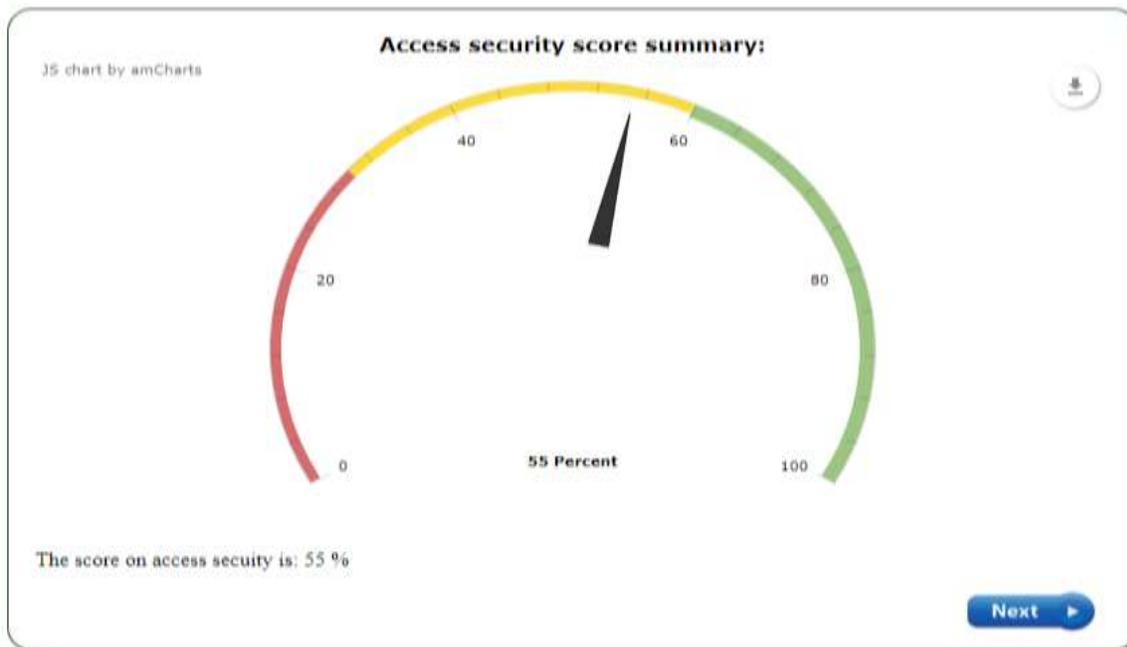
**Table 4.19: Access Control Measurement**

*Scale based rating for the performance levels of IT Security Elements*

For the tables below, please rate your response in a scale of 1 – 5, where, 1 = (Very ineffective), 2 = Ineffective), 3 = (Moderately Effective), 4 = (Effective), 5 = (Very Effective). You are requested to indicate the performance levels of IT security based on the elements below:

<i>Element four:</i>	<i>Access Control</i>	1	2	3	4	5
1	To what extent do you control access from external networks?	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2	have web content filtration?	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
3	have control of access from internal networks?	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4	well configured active directory and user-groups?	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

The dashboard then loads.....



**Table 4.20: Data Security Measurement**

*Scale based rating for the performance levels of IT Security Elements*

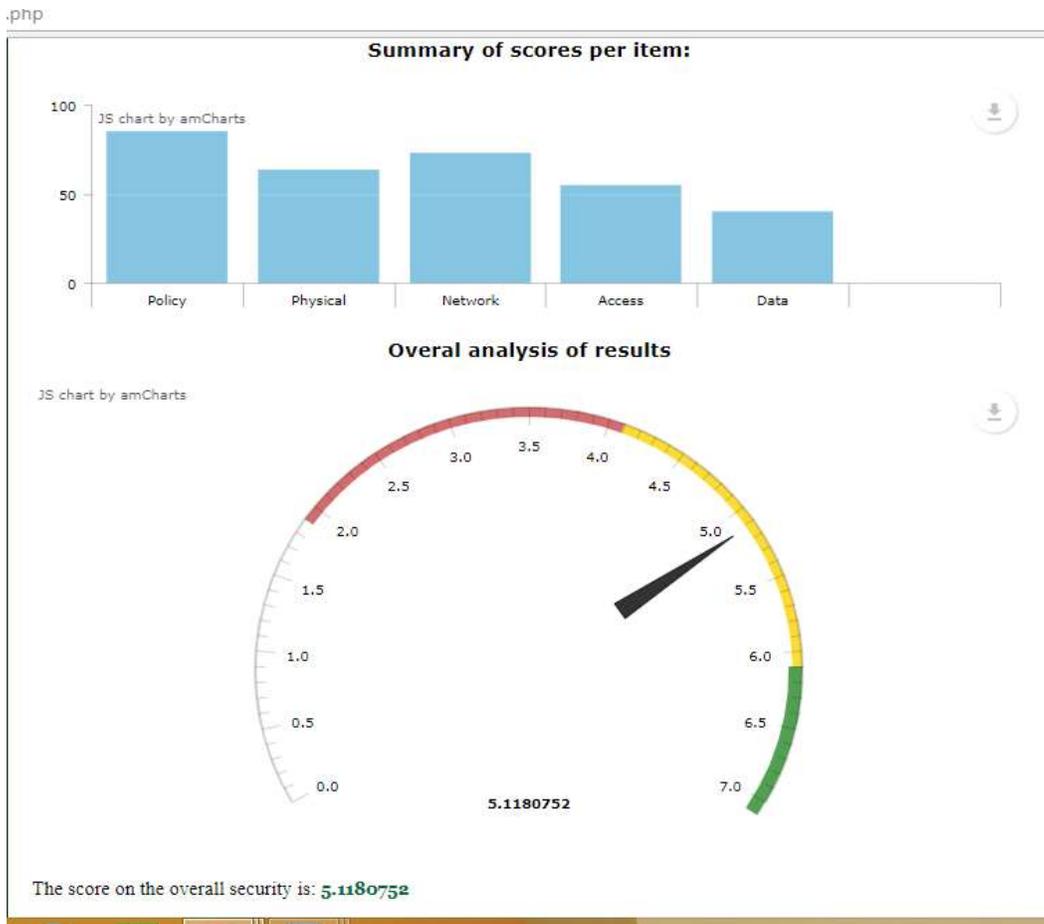
For the tables below, please rate your response in a scale of 1 – 5, where, 1 = (Very ineffective), 2 = Ineffective), 3 = (Moderately Effective), 4 = (Effective), 5 = (Very Effective). You are requested to indicate the performance levels of IT security based on the elements below.

	<i>Element five:</i>	<i>data security</i>				
<i>What is the:-</i>		<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>
<i>1</i>	<i>Level of encryption of electronic files in databases and storage?</i>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<i>2</i>	<i>Level of access control to functional data / databases?</i>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<i>3</i>	<i>Level of successful Data backup?</i>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<i>4</i>	<i>Level of successful Data restoration?</i>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<i>5</i>	<i>Level of malware control on systems holding data?</i>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<i>6</i>	<i>Level of entire systems back - up as hot site?</i>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<i>7</i>	<i>Level of Availability of critical servers and applications?</i>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<input type="button" value="Cancel"/>		<input type="button" value="Submit"/>		

The dashboard then loads.....



The overall assessment result for the IT security loads. This summarizes the implementation levels and thus measure the status of IT security based on the scores for all the elements in a given university. The overall metrics' value must fall between 1.9 (min) and 6.7 (max).



### Interpretation of Information on Tables 4.15 - 4.20

Through the dash-board of the developed IT security metric' model, the sub-elements constituting each major element are measured in percentage according to their levels of implementation, then the resultant values are quantified using regression model to produce a metrics value of range between 2.0 to 7.0.

## **CHAPTER FIVE**

### **CONCLUSION AND RECOMMENDATIONS**

#### **5.0 Introduction**

Here, the researcher draws conclusions, gives recommendations and proposes areas for further research consequent to the study. IT security management in most universities in Kenya has been without metrics, whereby management invests, but without clear ways of determining improvement of IT security status after such investments. The current method for estimating IT security in the university status rarely involve the application of the major elements of IT security, yet studies indicate that the elements could be important in determination of IT security metrics. The purpose of this research was to investigate the major elements of IT security and to apply the elements in determining a model for IT security metrics in universities in Kenya.

#### **5.1 Limitations and De-Limitations**

The major limitations identified in this study included: the study was limited to the universities in Kenya, and as such, the findings may not be generalized to other institutions of higher learning; the limits associated with the analytical approach partly based on regression analysis that could only determine correlation between the major IT security elements and metrics, but not causation aspects of the relationship; the inaccuracies inherent in GQM method, which is characterized by laborious expert estimation for preparing detailed goals, the corresponding questions and answers, as well as setting weight for every element of IT security. The de-limitations in the study were, firstly, the causation aspect for the relationship between the variables was found inconsequential in the metrics' model development. Secondly, the estimation challenge associated with GQM was overcome through the use of automated dashboard estimation platform in the metrics' dashboard. Further, both private and public universities were involved in the study to give a broader scope.

#### **5.2 Implications for Practice**

The IT security metrics model and its dashboard presentation on the online platform can be applied by IT security managers to improve IT security in their organizations. The metrics platform being simple enough can be used by institutional manager to gauge improvements made after investments on IT security appliances. Finally, the general public can access and use the online platform to estimate IT security status of their computerized institutions.

## **5.3 CONCLUSIONS**

### **5.3.1 Major IT Security Elements**

In relation to the objective one of the study, the study found that while the major IT security elements are applied in managing IT security within universities in Kenya, IT security policy plays more important role in IT security management within the universities. Physical security included signage implementation, control of systems asset register control, access to physical facilities as well as monitoring of physical facilities in their locations. Network security consists mainly of internet bandwidth supply, networks' structure, security tests, backbone – redundancy, Wi-Fi security controls as well as user-groups. Data security includes data back-up, data retrieval, malware control server unavailability data encryption as well as data classification. Finally, access control element was mainly concerned with password expiry, system authentication, physical intervention as well as network control access.

### **5.3.2 Relationship Between the Major IT Security Elements and IT Security Metrics**

For objective two of the research and considering the relationship between the major IT security elements and IT security metrics used in the universities, and showed that there is statistically significant association between the IT security elements and IT security metrics.

### **5.3.3 The Suitable IT Security Metric's Model Based on Major IT Security Elements**

For objective three, the suitable IT security metric's model based on major IT security elements for universities in Kenya was found to be  $Q_M = 1.904 + 1.62 SP + 0.800 PS + 0.808 NS + 0.796$

DS + 0.788 AC + E and this defined the model for IT security metrics. This model was interpreted that for a unit increase in every major IT security element, a significant increase in IT security metrics' value is predicted. Holding all other IT security elements' variables constant, the increase in IT security metrics associated with a unit increase of the element under consideration equals the coefficient value of the element under consideration. The simplified form of the model –  $Q_M = 1.9 + 0.8 (2 SP + PS + NS + DS + AC) + E$  yielded a unique model coefficient ratio of (2: 1). That is, the coefficient associated with IT security policy is twice as any other element in the model. This means IT security policy takes a cornerstone value in managing IT security. The above model was mounted online through the URL (<http://41.89.203.228/oguk>). This is a contribution to new knowledge in IT security.

#### **5.3.4 Applicability of the Developed IT Security Metrics' Model**

The study tested the applicability of the model in estimation of the prevailing IT security status for universities. The model was hosted on a local server at Rongo university server – room. The server is configured with a public IP address to facilitate international access through the internet via (<http://41.89.203.228/oguk>). The link leads to the online IT security metrics dashboard, such that when one clicks (<http://41.89.203.228/oguk>), the dash board provides an interactive platform for estimating the prevailing IT security status.

### **5.4 RECOMMENDATIONS**

It is recommended that:

1. IT security officers in universities single out each major IT security element and properly implement it for better systems' security management.
2. IT security policy be given much higher priority as it is the cornerstone for IT security management.
3. Universities should apply the knowledge of the highlighted network security elements and the practices to enhance network and the general information systems' management.
4. IT managers improve the status of IT security in their various institutions by implementing IT security appliances along the major IT security elements.

5. the developed online IT security model be used by institutions to help them in assessing their IT security status, especially before and after investment in IT security.
6. IT security trainers should, make their training modules better by incorporating network security elements and practices in their training packages.

#### **5.4.1 Policy Recommendations.**

It is recommended that:

1. IT security policy makers incorporate metrics in management of IT security.
2. Universities should develop and use of IT security policy for better information systems' security and governance.
3. Much more effort ought to be put in formulating, implementing and sensitizing the users about the IT security policy for better IT security management.
4. The resultant metrics model should be put to use by institutions for determining IT security situation, estimating returns on any investment in IT security and for general auditing of IT security health in line with implementation levels of the major elements of IT security.

#### **5.4.2 Recommendations for Further Research.**

The current study and the reviewed literature address a range of pertinent issues relating to IT security metrics and IT security elements' management within universities in Kenyan. Nevertheless, the debate on IT security measurement in general continues at accelerated rate, both in media domains and at scholarly levels, as well as at local and global levels. This shows that the field of IT security, especially IT security metrics needs more consideration and further research in other non-academic institutions. Findings of this study may not be conclusive in general, as they are only confined to administrative and user levels of ICT within the realms of universities in Kenyan. The universities may not be representative of all other institutions, like the non academic institutions as well as other cadres of institutions of learning like high schools, youth polytechnics, middle level college and dissimilar corporate organizations where ICT infrastructure is well developed.

The sampling approach, and the statistical analysis used may also have limitations. It would therefore, be desirable to further the study by using other methods and including comparative data from ICT users and administrators from other institutions. The inclusion of more institutions in a similar research would also merit further research. The study indicated that over 74% of the personnel working in the universities as either IT system technicians or users are male, with only less than 26% as of the female gender. This indicates that information technology field is still dominated much by the male gender, and there is therefore a need to conduct a further study on factors contributing to this observation. Since IT security policy was found to contribute more than other elements in the metrics' model, yet there is inadequate implementing of the policy, a study relating IT security policy implementation and breach of information systems should be conducted within the universities. Finally, a study should be done on systems sensors that can detect the implementation levels each element so that data input to the model is automated in real time.

## REFERENCES

- Abonyo, J. A. (2016). Mitigating and Dealing with Disasters: The Task of the Newly Information Manager in Knowledge Preservation. *Journal of Library and Information Sciences*, 4(1), 102-115.
- Abuya, T., Warren, C. E., Miller, N., Njuki, R., Ndwiga, C., Maranga, A., ... & Bellows, B. (2015). Exploring the prevalence of disrespect and abuse during childbirth in Kenya. *PloS one*, 10(4).
- Alhazmi, O. H., Malaiya, Y. K., & Ray, I. (2007). Measuring, analyzing and predicting security vulnerabilities in software systems. *Computers & Security*, 26(3), 219-228.
- Ahlgren, B., Dannewitz, C., Imbrenda, C., Kutscher, D., & Ohlman, B. (2012). A survey of information- centric networking. *IEEE Communications Magazine*, 50(7).
- Al-Ahmad, W., & Mohammad, B. (2013). Addressing information security risks by adopting standards. *International Journal of Information Security Science*, 2(2), 28-43.
- Armitage, C. J., & Conner, M. (2001). Efficacy of the theory of planned behaviour: A meta-analytic review. *British journal of social psychology*, 40(4), 471-499.
- Axelsson, S. (2000). *Intrusion detection systems: A survey and taxonomy* (Vol. 99). Technical report.
- Ampatzoglou, A., Ampatzoglou, A., Chatzigeorgiou, A., & Avgeriou, P. (2015). The financial aspect of managing technical debt: A systematic literature review. *Information and Software Technology*, 64, 52-73.
- Anderson, J. M. (2001). Why we need a new definition of information security. *Computers & Security*, 22(4), 308-313.
- Angelini, M., & Santucci, G. (2015). Visual cyber situational awareness for critical infrastructures. In *Proceedings of the 8th International Symposium on Visual Information Communication and Interaction* (pp. 83-92). ACM.
- Arora, V. (2010). Comparing different information security standards: COBIT v s. ISO 27001. *Qatar: Carnegie Mellon University*.
- Audebert, Y., & Le Saint, E. (2002). *U.S. Patent Application No. 10/085,127*.
- Azuwa, M. P., Ahmad, R., Sahib, S., & Shamsuddin, S. (2012). A propose technical security metrics model for SCADA systems. In *Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on* (pp. 70-75). IEEE.

- Babbie, E. R. (1998). *The practice of social research*. International Thomson Publishing Services.
- Ballou, B., Heitger, D. L., & Donnell, L. (2010). Creating effective dashboards. *Strategic Finance*, 91(9), 27.
- Barrett, C. B., Bezuneh, M., & Aboud, A. (2001). Income diversification, poverty traps and policy shocks in Côte d'Ivoire and Kenya. *Food policy*, 26(4), 367-384.
- Bichanga, O. W., & Obara, O. B. (2014). Challenges Facing Information Systems Security Management in Higher Learning Institutions: A Case Study of the Catholic University of Eastern Africa-Kenya. *International Journal of Management Excellence*, 3(1), 336-349.
- Bajaj, S., & Sion, R. (2014). Trusteddb: A trusted hardware-based database with privacy and data confidentiality. *IEEE Transactions on Knowledge and Data Engineering*, 26(3), 752-765.
- Bartol, N., Bates, B., Goertzel, K. M., & Winograd, T. (2009). Measuring cyber security and information assurance: a state-of-the-art report. Information Assurance Technology Analysis Center IATAC.
- Banerjee, A., Banerjee, C., Pandey, S. K., & Poonia, A. S. (2016). Development of iMACOQR Metrics Framework for Quantification of Software Security. In Proceedings of Fifth International Conference on Soft Computing for Problem Solving (pp. 711-719). Springer, Singapore.
- Beas, M. I., & Salanova, M. (2006). Self-efficacy beliefs, computer training and psychological well-being among information and communication technology workers. *Computers in Human Behavior*, 22(6), 1043-1058.
- Beaubouef, T., Petry, F. E., & Arora, G. (1998). Information-theoretic measures of uncertainty for rough sets and rough relational databases. *Information Sciences*, 109(1-4), 185-195.
- Bellare, M., Keelveedhi, S., & Ristenpart, T. (2013). DupLESS: Server-Aided Encryption for Deduplicated Storage. *IACR Cryptology ePrint Archive*, 2013, 429.
- Bessette, D., LeClair, J. A., Sylvertooth, R. E., & Burton, S. L. (2015). Communication, Technology, and Cyber Crime in Sub-Saharan Africa. *New Threats and Countermeasures in Digital Crime and Cyber Terrorism*, 286
- Bevans, B. (2016). Categorizing Blog Spam.
- Bichanga, O. W., & Obara, O. B. (2014). Challenges Facing Information Systems Security Management in Higher Learning Institutions: *Int. J. Management Excellence*, 3, 336-349.

- Bishop, M. (2003). What is computer security?. *IEEE Security & Privacy*, 1(1), 67-69.
- Black, P. E., Scarfone, K., & Souppaya, M. (2008). Cyber security metrics and measures. *Wiley Handbook of Science and Technology for Homeland Security*, 1-15.
- Blank, A., & Schiedel, L. (2003). *U.S. Patent Application No. 10/135,188*.
- Böhme, R. (2010, November). Security Metrics and Security Investment Models. In *IWSEC* (pp. 10-24).
- Bojanc, R., & Jerman-Blažič, B. (2013). A quantitative model for information-security risk management. *Engineering Management Journal*, 25(2), 25-37.
- Bond, T., & Fox, C. M. (2015). *Applying the Rasch model: Fundamental measurement in the human sciences*. Routledge.
- Boyer, W., & McQueen, M. (2007, October). Ideal based cyber security technical metrics for control systems. In *International Workshop on Critical Information Infrastructures Security* (pp. 246-260).
- Breier, J., & Hudec, L. (2011). Risk analysis supported by information security metrics. In *Proceedings of the 12th International Conference on Computer Systems and Technologies* (pp. 393-398). ACM.
- Brickell, E. F., Hall, C. D., Cihula, J. F., & Uhlig, R. (2011). *U.S. Patent No. 7,908,653*. Washington, DC: U.S. Patent and Trademark Office.
- Briggs, L. (2007). Tackling wicked problems: A public policy perspective. *Canberra: Australian Government, Commonwealth of Australia*.
- Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). An analysis. In *Proceedings of the Fourth European Conference on Software Architecture: Companion Volume* (pp. 189-196). ACM.
- Broadbent, J. (2007). If you can't measure it, how can you manage it? Management and governance in higher educational institutions. *Public Money and Management*, 27(3), 193-198.
- Broadbent, (2007, December). Information-theoretic security without an honest majority. In *International Conference on the Theory and Application of Cryptology and Information Security* (pp. 410-426).
- 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.

- Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic press.
- Calder, A., & Watkins, S. (2008). *IT governance: A manager's guide to data security and ISO 27001/ISO 27002*. Kogan Page Ltd.
- Chan, H., & Mubarak, S. (2012). Significance of information security awareness in the higher education sector. *International Journal of Computer Applications*, 60(10).
- Chang, V., Kuo, Y. H., & Ramachandran, M. (2016). Cloud computing adoption framework: A security framework for business clouds. *Future Generation Computer Systems*, 57, 24-41.
- Chin, E., Felt, A. P., Sekar, V., & Wagner, D. (2012). Measuring user confidence in smartphone security and privacy. In *Proceedings of the eighth symposium on usable privacy and security* (pp. 1-16).
- Chi, S., Park, J., Jung, K., & Lee, J. (2001). Network security modeling and cyber attack simulation methodology. In *Information Security and Privacy* (pp. 320-333). Springer Berlin/Heidelberg.
- Clogg, C. C. (1979). Some latent structure models for the analysis of Likert-type data. *Social Science Research*, 8(4), 287-301.
- Colombier, B., & Bossuet, L. (2014). Survey of hardware protection of design data for integrated circuits and intellectual properties. *IET Computers & Digital Techniques*, 8(6), 274-287.
- Costan, V., Lebedev, I. A., & Devadas, S. (2016). Sanctum: Minimal Hardware Extensions for Strong Software Isolation. In *USENIX Security Symposium* (pp. 857-874).
- Creswell, J. W., & Clark, V. L. P. (2017). *Designing and conducting mixed methods research*. Sage publications
- Daya, . (2013). Network security: History, importance, and future. *University of Florida Department of Electrical and Computer Engineering*.
- Delimitrou, C., & Kozyrakis, C. (2014, February). Quasar: resource-efficient and QoS-aware cluster management. In *ACM SIGPLAN Notices* (Vol. 49, No. 4, pp. 127-144). ACM.
- Deloitte, L. L. P. (2011). Mobile telephony and taxation in Kenya. *Nairobi: Deloitte LLP*.
- DeVellis, R. F. (2016). *Scale development: Theory and applications* (Vol. 26). Sage publications.

- Dhillon, G. (2007). *Principles of information systems security: Texts and cases*. John Wiley & Sons Incorporated.
- Doherty, N. F., Anastasakis, L., & Fulford, H. (2009). The information security policy unpacked: A critical study of the content of university policies. *International Journal of Information Management*, 29(6), 449-457
- Dworkin, M. J. (2016). *Recommendation for block cipher modes of operation: The CMAC mode for authentication* (No. Special Publication (NIST SP)-800-38B).
- Dworkin, M. J. (2016). Recommendation for block cipher modes of operation: The CMAC mode for authentication. Special Publication (NIST SP)-800-38B.
- Durkheim, E. (2013). *Professional ethics and civic morals*. Routledge.
- Dua, R., Raja, A. R., & Kakadia, D. (2014, March). Virtualization vs containerization to support paas. In *Cloud Engineering (IC2E), 2014 IEEE International Conference on* (pp. 610- 614). IEEE.
- Duncan, B., & Whittington, M. (2014). Compliance with standards, assurance and audit: Does this equal security?. In *Proceedings of the 7th International Conference on Security of Information and Networks* (p. 77). ACM
- Dunham, K., Hartman, S., Quintans, M., Morales, J. A., & Strazzere, T. (2014). *Android Malware and Analysis*. CRC Press.
- Elias, T. (2011). Learning analytics. *Learning*.
- Eira, J. P., & Rodrigues, A. J. (2009). Analysis of WiMAX data rate performance. Lisbon: Instituto de Telecomunicações/Instituto Superior, Technical University of Lisbon.
- Eschelbeck, G., & Villa, A. (2003). *U.S. Patent No. 6,611,869*. Washington, DC: U.S. Patent and Trademark Office.
- Evtushkin, D., Elwell, J., Ozsoy, M., Ponomarev, D., Ghazaleh, N. A., & Riley, R. (2014). Iso-x: A flexible architecture for hardware-managed isolated execution. In *Proceedings of the 47th Annual IEEE/ACM International Symposium on Microarchitecture* (pp. 190-202). IEEE Computer Society.
- Fenz, S., Heurix, J., & Neubauer, T. (2015). How to Increase the Inventory Efficiency i n Information Security Risk and Compliance Management. In *Proceedings of the European Conference on Information Systems (ECIS) 2015* (pp. 1-12). AIS}.
- Fernandes, D. A., Soares, L. F., Gomes, J. V., Freire, M. M., & Inácio, P. R. (2014). Security issues in cloud environments: a survey. *International Journal of Information Security*, 13(2), 113-170.

- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly: Management Information Systems*.
- Rabah, K. (2018). Convergence of AI, IoT, Big Data and Blockchain: A Review. *The Lake Institute Journal*.
- Filonik, D., Medland, R., Foth, M., & Rittenbruch, M. (2013). A customisable dashboard display for environmental performance visualisations. In *International Conference on Persuasive Technology* (pp. 51-62). Springer, Berlin, Heidelberg.
- Furnell, S. M., Bryant, P., & Phippen, A. D. (2007). Assessing the security perceptions of personal Internet users. *Computers & Security*, 26(5), 410-417.
- Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*.
- Galliers, R. D., & Leidner, D. E. (Eds.). (2014). *Strategic information management: challenges and strategies in managing information systems*. Routledge.
- Gamal, M. M., Hasan, B., & Hegazy, A. F. (2011). A security analysis framework powered by an expert system. *International Journal of Computer Science and Security (IJCSS)*, 4(6), 505-527.
- Gawronski, B., & Payne, B. K. (Eds.). (2011). *Handbook of implicit social cognition: Measurement, theory, and applications*. Guilford Press.
- Gay, P. (2001). *Weimar culture: the outsider as insider*. WW Norton & Company.
- Gerber, M., & Von Solms, R. (2008). Information security requirements—interpreting the legal aspects. *Computers & Security*, 27(5), 124-135.
- Gesmann, M., & de Castillo, D. (2011). Using the Google visualisation API with R. *The R Journal*, 3(2), 40-44.
- Gibson, G. A., & Van Meter, R. (2000). Network attached storage architecture. *Communications of the ACM*, 43(11), 37-45.
- Goff, S., & ProjectExperts, C. E. O. (2008). Everything I Know Today About Project Time Management I Learned In Sports Car Racing.
- Gleichauf, R. E., Teal, D. M., & Wiley, K. L. (2002). *U.S. Patent No. 6,499,107*. Washington, DC: U.S. Patent and Trademark Office.
- Glewwe, P., Kremer, M., & Moulin, S. (2009). Many children left behind? Textbooks and test scores in Kenya. *American Economic Journal: Applied Economics*, 1(1), 112-35.

- Grama, J. (2014). Just in Time Research: Data Breaches in Higher Education. *EDUCAUSE*.
- Gravetter, F. J., & Forzano, L. A. B. (2003). *Research methods for the behavioral sciences*. Thomson.
- Gritzalis, D., Kandias, M., Stavrou, V., & Mitrou, L. (2014). History of information: the case of privacy and security in social media. In *Proc. of the History of Information Conference* (pp. 283-310).
- Gollmann, D., & Meier, J. (2006). *Computer Security—ESORICS 2006: 11th European Symposium on Research in Computer Security, Hamburg, Germany, September 18-20, 2006, Proceedings* (Vol. 4189). Springer Science & Business Media.
- Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems*, 29(7), 1645- 1660.
- Haubner, G., Petermann, H., & Zobl, H. (1986). *U.S. Patent No. 4,630,043*. Washington, DC: U.S. Patent and Trademark Office.
- Houngbo, P. J., & Hounsou, J. T. (2015). Measuring Information Security: Understanding And Selecting Appropriate Metrics. *International Journal of Computer Science and Security (IJCSS)*, 9(2), 108.nature of groups engaged in cyber crime
- Howe, E. D. (2015). *Mormonism unveiled* (p. 252). Utah Lighthouse Ministry.
- Huber, K. D., Flynn, J. J., & Mansfield, W. G. (2016). *U.S. Patent No. 9,319,964*. Washington, DC: U.S. Patent and Trademark Office.
- Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, 43(4), 615-660.
- Ismail, R., & Zainab, A. N. (2013). Information systems security in special and public libraries: an assessment of status. *arXiv preprint arXiv:1301.5386*.
- Jaffer, S., Ng'ambi, D., & Czerniewicz, L. (2007). The role of ICTs in higher education in South Africa: One strategy for addressing teaching and learning challenges. *International journal of Education and Development using ICT*, 3(4).

- Jagadeeshwar, M., Shriramoju, S. K., & Babu, A. R. (2016). Optimal Distributed Malware Defense in Mobile Networks with Heterogeneous Devices.
- Jansen, W. (2010). *Directions in security metrics research*. Diane Publishing.
- Jaquith, A. (2007). Security metrics: replacing fear, uncertainty, and doubt(Vol. 36). Upper Saddle River: Addison-Wesley.
- Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the internet of things: Johnson, C. N. (2002). The benefits of PDCA. *Quality Progress*, 35(5), 120.
- Jonsson, E., & Pirzadeh, L. (2011). A framework for security metrics based on operational system attributes. In 2011 Third International Workshop on Security Measurements and Metrics (pp. 58-65). IEEE.
- Johnson, A., (2002). Managers at Work: How Six Sigma Improves R&D. *Research-Technology Management*, 46(2), 12-15.
- Jordan, S. M., McMahon, P. W., McNeill, D. B., & Panlilio-Yap, N. M. (2005). *U.S. Patent No. 6,968,312*. Washington, DC: U.S. Patent and Trademark Office.
- Kamerman, A., Monteban, L., & Mud, R. (2000). *U.S. Patent No. 6,067,291*. Washington, DC: U.S. Patent and Trademark Office.
- Kancharla, P., & Manapragada, R. K. (2014). *U.S. Patent Application No. 14/299,739*.
- Kanstrén, T., Savola, R., Evesti, A., Pentikäinen, H., Hecker, A., Ouedraogo, M., ... & Ros, S. (2010). Towards an abstraction layer for security assurance measurements.
- Kankanhalli, A., Teo, H. H., Tan, B. C., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International journal of information management*, 23(2), 139-154.
- Kiilu, C. P. K., & Nzuki, D. M. (2014) *Factors Affecting Adoption of Information Security Management Systems: A Theoretical Review*.
- Kitheka, P. M. (2013). Information Security Management Systems In Public Universities In Kenya: A Gap Analysis between Common Practices and Industry Best Practices (Doctoral dissertation, University of Nairobi).
- Kimwele, M., Mwangi, W., & Kimani, S. (2011). Information technology (IT) security framework for Kenyan small and medium enterprises (SMEs). *Int. J. Comput. Sci. Secur. IJCSS*, 5(1), 39.
- Kiresuk, T. J., Smith, A., & Cardillo, J. E. (2014). *Goal attainment scaling: Applications, theory, and measurement*. Psychology Press.

- Kombo, D. K., & Tromp, D. L. (2006). Proposal and thesis writing: An introduction. *Nairobi: Paulines Publications Africa*, 10-45.
- Kothari, C. R. (2003). Research Methodology–Methods & Techniques, Wishawa Prakashan, New Delhi. *Ali SS, Models in Consumer Buying Behaviour, Deep & Deep Publications*.
- Krombholz, K., Frühwirt, P., Rieder, T., Kapsalis, I., Ullrich, J., & Weippl, E. (2015). QR Code Security--How Secure and Usable Apps Can Protect Users Against Malicious QR Codes. In *Availability, Reliability and Security (ARES), 2015 10th International Conference on* (pp. 230-237). IEEE.
- Kruczkowski, M., & Niewiadomska-Szynkiewicz, E. (2014). Comparative study of supervised learning methods for malware analysis. *Journal of Telecommunications and Information Technology*, (4), 24.
- Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *computers & security*, 25(4), 289-296.
- Lane, T. (2007) "Information security management in Australian Universities: An exploratory analysis." (2007).
- Lebel, P. (2007). *U.S. Patent Application No. 11/212,790*.
- Lenders, V., Tanner, A., & Blarer, A. (2015). Gaining an edge in cyberspace with advanced situational awareness. *IEEE Security & Privacy*, 13(2), 65-74.
- Lennon, E. B., Swanson, M., Sabato, J., Hash, J., Graffo, L., & Sp, N. (2003). IT security metrics. *ITL Bulletin, National Institute of Standards and Technology*.
- Lingard, H., Wakefield, R., & Blismas, N. (2013). "If you cannot measure it, you cannot improve it": Measuring health and safety performance in the construction industry. In *the 19th Triennial CIB World Building Congress, Queensland University of Technology,, Brisbane, Queensland, Australia*.
- Lin, W. C., Ke, S. W., & Tsai, C. F. (2015). CANN: An intrusion detection system based on combining cluster centers and nearest neighbors. *Knowledge-based systems*, 78, 13-21.
- Lie, H. W., & Bos, B. (2005). *Cascading style sheets: designing for the Web*. Addison-Wesley Professional.
- Lodgaard, E., & Aasland, K. E. (2011). An examination of the application of plan-do-check-act cycle in product development. In *DS 68-10: Proceedings of the 18th International Conference on Engineering Design (ICED 11), Impacting Society through Engineering Design, Vol. 10: Design Methods and Tools pt. 2, Lyngby/Copenhagen, Denmark, 15.-19.08. 2011*.

- Lukman, R., Krajnc, D., & Glavič, P. (2010). University ranking using research, educational and environmental indicators. *Journal of Cleaner Production*, 18(7), 619-628.
- Luambano, I., & Nawe, J. (2004). Internet use by students of the University of Dar es Salaam. *Library Hi Tech News*, 21(10), 13-17.
- Mathieson, K. (1991). Predicting user intentions: comparing the technology acceptance model with the theory of planned behavior. *Information systems research*, 2(3), 173-191.
- Macrae, D. (2003). *U.S. Patent Application No. 10/196,583*.
- MacLean, R. (2012). Dangerous environments. *Environmental Quality Management*, 21(3), 109-116.
- Makori, E. (2013). Adoption of radio frequency identification technology in university libraries: A Kenyan perspective. *The Electronic Library*, 31(2), 208-216.
- Mahnic, V., Uratnik, J., & Zabkar, N. (2002). *Information security of university information systems* (pp. 97-105). GI.
- Mang'ira, R., & Andrew, K. (2014). Towards establishment of a full-fledged disaster management department for Moi University libraries.
- Martin, R. A. (2008). Making security measurable and manageable. In *Military Communications Conference, 2008. MILCOM 2008. IEEE* (pp. 1-9). IEEE.
- Martins, A., Eloff, J. H. P., & Park, A. (2001). Measuring information security. In *Proceedings of Workshop on Information Security–System Rating and Ranking*.
- Mashiko, Y., & Basili, V. R. (1997). Using the GQM paradigm to investigate influential factors for software process improvement. *Journal of Systems and Software*, 36(1), 17-32.
- Matthews, B., & Ross, L. (2014). *Research methods*. Pearson Higher Ed.
- May, C. (2003). Dynamic corporate culture lies at the heart of effective security strategy. *Computer Fraud & Security*, 2003(5), 10-13.
- McNamara, B. (2015). Airbnb: A not-so-safe resting place. *J. on Telecomm. & High Tech. L.*, 13, 149.
- Mingaine, L. (2013). Skill challenges in adoption and use of ICT in public secondary schools, Kenya. *International Journal of Humanities and Social Science*, 3(13), 61-72.

- Mitnick, K. D., & Simon, W. L. (2011). *The art of deception: Controlling the human element of security*. John Wiley & Sons.
- Mohlabeng, M. R., Mokwena, S. N., & Osunmakinde, I. O. (2012). Towards Implementation of the Information Security Strategies in South Africa. *Journal of Emerging Trends in Computing and Information Sciences*, 3(11).
- Mong'eri, M. K. (2014). *Security in health workforce information systems: a case of regulatory human resource information system* (Doctoral dissertation, University of Nairobi).
- Mugenda, O. & Mugenda A. (2003). *Research methods: quantitative and qualitative approaches*.
- Mukhwana, E. J., Kande, A., & Too, J. (2017). Transforming University Education in Africa: Lessons from Kenya. *African Journal of Rural Development*, 2(3), 341-352.
- Muijs, D. (2010). *Doing quantitative research in education with SPSS*. Sage.
- Murugesan, S., & Gangadharan, G. R. (2012). *Harnessing green IT: Principles and practices*. Wiley Publishing.
- Mulwa, A. S. (2012). The influence of institutional and human factors on readiness to adopt E-Learning in Kenya: The case of secondary schools in Kitui district. *An unpublished PhD thesis of the University of Nairobi*.
- Mullard, J. (2007). Corrosion-induced cover cracking: new test data and predictive models. *ACI Structural Journal*, 108(1), 71.
- Mwangi, W., & Kimani, S. (2011). Information technology (IT) security framework for Kenyan small and medium enterprises (SMEs). *Int. J. Comput. Sci. Secur. IJCSS*, 5(1), 39.
- Muus, K. J., Baker-Demaray, T., McDonald, L. R., Ludtke, R. L., Allery, A. J., Bogart, T. A., ... & Buchwald, D. S. (2009). Body mass index and cancer screening in older American Indian and Alaska Native men. *The Journal of Rural Health*, 25(1), 104-108.
- Mitnick, K. D., & Simon, W. L. (2011). *The art of deception: Controlling the human element of security*. John Wiley & Sons.
- Neto, A. A., & Vieira, M. (2010). Benchmarking Untrustworthiness: An Alternative to Security Measurement. *International Journal of Dependable and Trustworthy Information Systems (IJDTIS)*, 1(2), 32-54.

- Ndung'u, P. W., & Kyalo, J. K. (2015). An evaluation of enterprise resource planning systems implementation experiences for selected Public Universities in Kenya.
- Nixon, K. C. (2012). Winclada (BETA) ver. 0.9. 9. *Published by the author*.
- Nyamongo, D. M. (2012). *Information systems security management* (Doctoral dissertation, Strathmore University).
- Nweze, C. M. (2010). The use of ICT in Nigerian universities: A case study of Obafemi Awolowo University, Ile-Ife.
- NIST : Mell, P., (2009). The NIST definition of cloud computing.
- O'Flynn, C., & Chen, Z. D. (2014). Chipwhisperer: An open-source platform for hardware embedded security research. In *International Workshop on Constructive Side-Channel Analysis and Secure Design* (pp. 243-260). Springer, Cham.
- Olden, E. M. (2002). *U.S. Patent No. 6,460,141*. Washington, DC: U.S. Patent and Trademark Office.
- Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: an example, design considerations and applications. *Information & management*, 42(1), 15-29.
- Okibo, B. W., & Ochiche, O. B. (2014). Challenges Facing Information Systems Security Management in Higher Learning Institutions: A Case Study of the Catholic University of Eastern Africa-Kenya. *International Journal of Management Excellence*, 3(1), 336-349.
- O'Mahony, M., & Timmer, M. P. (2009). Output, input and productivity measures at the industry level: the EU KLEMS database. *The Economic Journal*, 119(538).
- Ope, J. O. (2014). An information systems security framework for Kenyan public universities (Doctoral dissertation, University of Nairobi).
- O'neil, P. (2014). *DATABASE: principles programming performance*. Morgan Kaufmann.
- Okuku, A., Renaud, K., & Valeriano, B. (2015). Cybersecurity strategy's role in raising Kenyan awareness of mobile security threats. *Information & Security*, 32(2), 1.
- Oguk, C., Karie, N., & Rabah, K. (2017). Network Security Management in Universities in Kenya. *Mara Research Journal of Computer Science & Security*, 2(1), 48-60.
- Overy, M. R., & Sullivan, M. J. (2005). U.S. Patent No. 6,961,541. Washington, DC: U.S. Patent and Trademark Office.

- Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health and Mental Health Services Research*, 42(5), 533-544.
- Patriciu, V. V., Priescu, I., & Nicolaescu, S. (2006). Security metrics for enterprise information systems. *Journal of Applied Quantitative Methods*, 1(2), 151-159.
- Pasquini, A., & Galiè, E. (2013). COBIT 5 and the Process Capability Model. Improvements Provided for IT Governance Process. In *Proceedings of FIKUSZ'13 Symposium for Young Researchers* (pp. 67-76).
- Payne, S. C. (2006). A guide to security metrics. SANS Institute Information Security Reading Room.
- Peterson, L. L., & Davie, B. S. (2007). *Computer networks: a systems approach*. Elsevier.
- Peláez, M. H. S. (2010). Measuring effectiveness in Information Security Controls. SANS Institute InfoSec Reading Room, [http://www.sans.org/reading\\_room/whitepapers/basics/measuring-effectiveness-information-security-controls\\_33398](http://www.sans.org/reading_room/whitepapers/basics/measuring-effectiveness-information-security-controls_33398).
- Peltier, T. R. Tich, r.e, Yae, U., Polkh, w.(2005). Implementing an Information Security Awareness Program. *Information Systems Security*, 14(2), 37-49.
- Pfleeger, S. L., & Cunningham, R. K. (2010). Why measuring security is hard. *IEEE Security & Privacy*, 4(8), 46-54.
- Renaud, K., Blignaut, R., & Venter, I. (2016). Smartphone Owners Need Security Advice.
- Rajiv A.Y.,(2009). Transparency and accountability in NREGA: a case study of Andhra Pradesh.
- Ramsey, J., Ketts, K., & Buer, S. (2008). *U.S. Patent No. 7,331,061*. Washington, DC: U.S. Patent and Trademark Office.
- Reid, J. G., Carroll, A., Veeraraghavan, N., Dahdouli, M., Sundquist, A., English, A., ... & Yu, F. (2014). Launching genomics into the cloud: deployment of Mercury, a next generation sequence analysis pipeline. *BMC bioinformatics*, 15(1), 30.
- Rayes, A., & Cheung, M. (2007). *U.S. Patent No. 7,237,267*. Washington, DC: U.S. Patent and Trademark Office.
- Roh, W., Seol, J. Y., Park, J., Lee, B., Lee, J., Kim, Y., ... & Aryanfar, F. (2014). Millimeter-

- wave beamforming as an enabling technology for 5G cellular communications: Theoretical feasibility and prototype results. *IEEE communications magazine*, 52(2), 106-113.
- Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, 57(10), 2266-2279.
- Rostami, M., Koushanfar, F., & Karri, R. (2014). A primer on hardware security: Models, methods, and metrics. *Proceedings of the IEEE*, 102(8), 1283-1295.
- Rothermel, P. M., Bonn, D. W., & Marvais, N. T. (2004). *U.S. Patent No. 6,678,827*. Washington, DC: U.S. Patent and Trademark Office
- Roth, W. M., & Bowen, G. M. (2003). When are graphs worth ten thousand words? An expert-expert study. *Cognition and Instruction*, 21(4), 429-473.
- Rubin, A., & Babbie, E. R. (2012). *Brooks/Cole Empowerment Series: Essential research methods for social work*. Cengage Learning.
- Ryan, J. J., & Ryan, D. J. (2008). Performance metrics for information security risk management. *IEEE Security & Privacy*, 6(5).
- Sajid, A., Abbas, H., & Saleem, K. (2016). Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges. *IEEE Access*, 4, 1375-1384.
- SANS (2007). CloudAV: N-Version Antivirus in the Network Cloud. In *USENIX Security Symposium* (pp. 91-106).
- Sabah, F. (2011, May). Virtualization-level security in cloud computing. In *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on* (pp. 250-254). IEEE.
- Safer, A. (2012). A picture is worth a thousand words. *Marine Log*, 117-111.
- Saleh, M. S., & Bakry, S. H. (2008). An overview of key IT risk management methods. *Saudi Computer Journal*, 6(2), 61-70.
- Sadeghi, A. R., Wachsmann, C., & Waidner, M. (2015). Security and privacy challenges in industrial internet of things. In *Proceedings of the 52nd annual design automation conference* (p. 54). ACM.
- Sandvik, K. B. (2016). The humanitarian cyberspace: shrinking space or an expanding frontier?. *Third World Quarterly*, 37(1), 17-32.
- Sarantakos, S. (2012). *Social research*. Palgrave Macmillan.

- Sawazaki, J., Maeda, T., & Yonezawa, A. (2010, December). Implementing a hybrid virtual machine monitor for flexible and efficient security mechanisms. In Dependable Computing (PRDC), 2010 IEEE 16th Pacific Rim International Symposium on (pp. 37- 46). IEEE.
- Selwyn, N. (2007). The use of computer technology in university teaching and learning: a critical perspective. *Journal of computer assisted learning*, 23(2), 83-94.
- Seegar, M. (2005). U.S. Patent Application No. 11/253,180.
- Sekeres, M. A., & Bolwell, B. J. (2016). Will cancer patients be the next victims of the data privacy debate. *FoxNews.com*. Accessed April, 19.
- Shah, A., Novy, R. F., & Ertl, R. A. (2007). U.S. Patent No. 7,167,859. Washington, DC: U.S. Patent and Trademark Office.
- Shiple, P. M. (2000). U.S. Patent No. 6,119,236. Washington, DC: U.S. Patent and Trademark Office.
- Skidmore, R. R., & Rappaport, T. S. (2002). U.S. Patent No. 6,442,507. Washington, DC: U.S. Patent and Trademark Office.
- Shostack, A., & Allouch, D. (2001). *U.S. Patent No. 6,298,445*. Washington, DC: U.S. Patent and Trademark Office.
- Sheikhpour, R., & Modiri, N. (2012). An Approach to Map COBIT Processes to ISO/IEC 27001 Information Security Management Controls. *International Journal of Security and Its Applications*, 6(2), 13-28.
- Stott, B., Marinho, J. L., & Alsac, O. (1979). Review of linear programming applied to power system rescheduling. In *Power Industry Computer Applications Conference, 1979. PICA-79. IEEE Conference Proceedings* (pp. 142-154). IEEE.
- Shelc, R. (2015). Authorized Access and the Challenges of Health Information Systems.
- Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS quarterly*, 487-502.
- Sireci, S., & Faulkner-Bond, M. (2014). Validity evidence based on test content. *Psicothema*, 26(1), 100-107.
- Smith, S. (2013). Determining sample size: How to ensure you get the correct sample size. E-Book (c) Qualtrics Online Sample.

- Son, I., & Lee, D. (2011). Assessing A New IT Service Model, Cloud Computing. In PACIS (p. 179).
- Sonnenreich, W., Albanese, J., & Stout, B. (2006). Return on security investment (ROSI)-a practical quantitative model. *Journal of Research and practice in Information Technology*, 38(1), 45-56
- Stark, J. (2015). Product lifecycle management. In *Product Lifecycle Management (Volume 1)* (pp. 1-29). Springer International Publishing.
- Stojmenovic, I., & Wen, S. (2014). The fog computing paradigm: Scenarios and security issues. In *Computer Science and Information Systems (FedCSIS), 2014 Federated Conference on* (pp. 1-8). IEEE.
- Stott, B., & Marinho, J. L. (1979). Linear programming for power-system network security applications. *IEEE Transactions on Power Apparatus and Systems*, (3), 837-848.
- Stolfo, S., Bellovin, S. M., & Evans, D. (2011). Measuring security. *IEEE Security & Privacy*, 9(3), 60-65.
- Sveiby, K. E. (2001). Methods for measuring intangible assets.
- Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications*, 34(1), 1-11.
- Stallings, W., & Tahiliani, M. P. (2014). *Cryptography and network security: principles and practice* (Vol. 6). London: Pearson.
- Sridhar, S., & Govindarasu, M. (2014). Model-based attack detection and mitigation for automatic generation control. *IEEE Transactions on Smart Grid*, 5(2), 580-591.
- Stallings, W., & Brown, L. (2008). Computer security. *Principles and Practice*. Stallings & Brown, (2008).
- Suakanto, S., Supangkat, S. H., & Saragih, R. (2013). Smart city dashboard for integrating various data of sensor networks. In *ICT for Smart Society (ICISS), 2013 International Conference on* (pp. 1-5). IEEE.
- Sweet, W., & Yu, J. (2002). *U.S. Patent Application No. 09/930,029*.
- Tarus, J. K., Gichoya, D., & Muumbo, A. (2015). "Challenges of implementing e-learning in Kenya: A case of Kenyan public universities". *The International Review of Research in Open and Distributed Learning*, 16(1).
- Taylor, S., & Todd, P. A. (1995). Understanding information technology usage: A test of competing models. *Information systems research*, 6(2), 144-176.

- Tibenderana, P. K., & Ogao, P. J. (2008). Acceptance and use of electronic library services in Ugandan universities. In *Proceedings of the 8th ACM/IEEE-CS joint conference on Digital libraries* (pp. 323-332). ACM.
- Thornton, S. (2001). A picture is worth a thousand words. In *New ideas in mathematics education: Proceedings of the International Conference of the Mathematics Education into the 21st Century Project* (pp. 251-256).
- Thomas, T., Chu, B., Lipford, H., Smith, J., & Murphy-Hill, E. (2015). A study of interactive code annotation for access control vulnerabilities. In *Visual Languages and Human-Centric Computing (VL/HCC), 2015 IEEE Symposium on* (pp. 73-77). IEEE.
- Tipton, H., & Krause, M. (2000). Information security management.
- Toth, P., & Vigo, D. (Eds.). (2014). *Vehicle routing: problems, methods, and applications*. Society for Industrial and Applied Mathematics.
- Tracy, S. J. (2010). Qualitative quality: Eight “big-tent” criteria for excellent qualitative research. *Qualitative inquiry*, 16(10), 837-851.
- Trethowen, L., Anslow, C., Marshall, S., & Welch, I. (2015). VisRAID: Visualizing Remote Access for Intrusion Detection. In *Australasian Conference on Information Security and Privacy* (pp. 289-306). Springer International Publishing.
- Turner, A. G. (2003). Sampling strategies. *Handbook on designing of household sample surveys*. Geneva: United Nations Statistics Division.
- Tzu-Chin, R. (2016). A Scale of University Students' Attitudes toward e-Learning on the Moodle System. *International Journal of Online Pedagogy and Course Design (IJOPCD)*, 4(3), 49-65.
- Tomlinson, G. (2012). *U.S. Patent No. 8,255,973*. Washington, DC: U.S. Patent and Trademark Office.
- Thomas, J. R., Silverman, S., & Nelson, J. (2015). *Research methods in physical activity, 7E*. Human kinetics.
- Tongco, M. D. C. (2007). Purposive sampling as a tool for informant selection. *Ethnobotany Research and applications*, 5, 147-158.
- Tarus, D. K. (2015). Corporate social responsibility engagement in Kenya: Bottom line or rhetoric?. *Journal of African Business*, 16(3), 289-304.
- Union, A. (2014). Implementation Strategy and Roadmap to Achieve the 2025 Vision on CAADP. Addis Ababa: African Union.

- Vaarandi, R., & Pihelgas, M. (2014, October). Using security logs for collecting and reporting technical security metrics. In Military Communications Conference (MILCOM), 2014 IEEE (pp. 294-299). IEEE.
- Vacca, J. R. (2012). *Computer and information security handbook*. Newnes.
- Vaishnavi, V. K., & Kuechler, W. (2015). *Design science research methods and patterns: innovating information and communication technology*. Crc Press.
- Veseli, I. (2011). *Measuring the Effectiveness of Information Security Awareness Program* (Master's thesis).
- Verendel, V. (2009). Quantified security is a weak hypothesis: a critical survey of results and assumptions. In Proceedings of the 2009 workshop on New security paradigms workshop (pp. 37-50). ACM.
- Von Solms, S. B. (2005). Information Security Governance–compliance management vs operational management. *Computers & Security*, 24(6), 443-447.
- Walther, J. B., Slovacek, C. L., & Tidwell, L. C. (2001). Is a picture worth a thousand words? Photographic images in long-term and short-term computer-mediated communication. *Communication Research*, 28(1), 105-134.
- Wang, A. J. A. (2005). Information security models and metrics. In *Proceedings of the 43rd annual Southeast regional conference-Volume 2* (pp. 178-184). ACM. *Conference on the Theory and Application of Cryptology and Information Security*(pp. 410-426). Springer, Berlin, Heidelberg
- Whitson, G. (2003). Computer security: Theory, process and management. *Journal of computing sciences in colleges*, 18(6), 57-66.
- Wohlever, R., (2009). A solution to resource underutilization for web services hosted in the cloud. In *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"* (pp. 567-584). Springer, Berlin, Heidelberg.
- Zhang, S., & Le, Fever, (2013). An Examination of the Practicability of COBIT Framework and the Proposal of a COBIT-BSC Model. *Journal of Economics*, 1, 5.
- Zhu, J. (2015). *Optimization of power system operation* (Vol. 47). John Wiley & Sons.

## APPENDICES

### Appendix 1 : Questionnaire TYPE 1: for Information Systems Users Only

The purpose of this questionnaire is to facilitate collection of data that will be used in investigating the IT Security elements for developing IT security metrics in Universities in Kenya. The respondent should be at least a team-leader under each of the following: *students' finance, students' registration, examinations, human resources, audit, library, health facility, and computer laboratory.*

#### **SECTION A: General Information:**

1. Which category of university do you work for?  
Private  Public
2. Which department do you belong to? .....
3. What is your age group in years ? Under 30  30-40  41-50  above 50
4. Gender : Male  Female
5. Are you an IT systems **user** in the university ? Yes  No  (if No, don't continue)
6. Please state your highest level of education? Diploma  Degree  postgraduate
7. State your work experience in this university?  
Less than 3 years  3-6 years  over 6 years
8. How is the system security? Secure  Insecure  Not sure .

#### **SECTION B: Specific Information on the adoption of IT Security Elements in universities**

##### *User experience on Computer on IT Policy*

1. Do you have an IT security policy? Yes  No
2. To what extent do you feel the impact of IT security policy?  
low  Moderate  High
3. Do you know what the IT security policy requires on sharing user password?  
Yes  No

4. Are there well defined consequences for violating IT security policy?

Yes [ ] No [ ]

5. How often does the university train you on IT security?

Regularly [ ] Irregularly [ ] Never [ ]

6. Are employees sensitized on IT security requirements and practices?

Yes [ ] No [ ]

### ***Users experience on Physical Security***

1. Are there signage's (post marks) for IT resources e.g. labeled sign along fiber optics lines?

Yes [ ] No [ ]

2. Does the university effectively maintain IT systems asset register? Yes [ ] No [ ]

3. Is there control of access to physical facilities hosting IT systems Yes [ ] No [ ]

4. Is there monitoring of it facilities through CCTV Yes [ ] No [ ]

5. Does the university recover portable computing devices (e.g. university owned laptops, tablets and external storage media) from staff when they are leaving the organization?

Yes [ ] No [ ]

### ***User experience on Computer Network***

1. How fast is the internet? slow [ ] Moderate [ ] High [ ]

2. Are there controls against transferring information through portable devices ?

Yes [ ] No [ ]

3. How often do you experience total internet outage?

At most once a week [ ] Over twice a week [ ]

4. What is the requirement to access the Wi-Fi?

One password for all users [ ] *Unique* account and unique password [ ]

Other:.....

5. Are systems users configured into various user-groups? Yes [ ] No [ ]

6. Are there internet sites you cannot access from the university network? Yes [ ] No [ ]

### ***Users experience on Data Security***

**(I)**

1. Do you conduct data classification? Yes [ ] No [ ]
2. What is your most critical data?.....
3. Have you ever lost data in the system? Yes [ ] No [ ]
4. Have you ever recovered data that had been lost from the system? Yes [ ] No [ ]
5. How do you protect your data / systems against;
  - a. unauthorized access .....
  - b. unauthorized modification .....
  - c. data loss .....

**(II)**

***Response on ERP Experience***

- i. Has your ERP system been successfully implemented to completion? Yes [ ] No [ ]
- ii. Have you ever experienced a major security issue in the system? Yes [ ] No [ ]
- iii. Does the ERP /automation system give consistent reports? Yes [ ] No [ ]
- iv. Does the ERP / automation system have automated back-up system? Yes [ ] No [ ]
- v. Do you find ERP systems more efficient than non-integrated systems like "quick books"
 

Yes [ ] No [ ]
- vi. Have students ever attempted to change data through the ERP systems? Yes [ ] No [ ]
- vii. Do you have IT risk mitigation strategy? Yes [ ] No [ ]
- viii. Do you have disaster recovery plan and site? Yes [ ] No [ ]
- ix. Has your disaster recovery system ever been tested? Yes [ ] No [ ]
  - i. If Yes, How effective was it?
 

.....

***Users experience on Access Control***

1. How easy is it to access the server-room?
 

Easy [ ]      moderately difficult [ ]      very difficult [ ]
2. Is user grouping applied in managing systems' security? Yes [ ] No [ ]
3. Is system access limited to particular hours within the day / week? Yes [ ] No [ ]
4. How often do you change your password? .....
5. Do you operate on encrypted file and folders? Yes [ ] No [ ]

## Appendix 2 : Questionnaire type 2: for ICT Personnel Only

The purpose of this questionnaire is to facilitate collection of data that will be used in investigating IT Security elements as well as their relationship with metrics in Universities in Kenya.

*The respondents should be from areas related to: IT leadership, network administration, systems administration, IT security administration and database administration.*

### PART A: General Information

- a) Which category of university do you work for?
  - a. Private  Public
- b) Which Department do you belong?.....
- c) Gender: Male  Female
- d) What is your age group in years ? Under 30  30-40  41-50  above 50
- e) Are you IT Personnel?  Yes  No
- f) State your highest level of education? Diploma  Degree  postgraduate
- g) State your work experience in this university?
  - a. Less than 3 years  3-6 years  over 6 years
- h) Do you have formal training in information system security? Yes  No
- i) Do you have specialized training in ICT related security? Yes  No
- j) How is the university website security? Secure  Insecure  Not sure . Give reason for your choice.....

### PART B: Information on ICT Infrastructure and the elements of IT security

#### (I)

- i. Is ICT security audit conducted regularly in your systems?  Yes  No
- ii. Is your server (database, systems) attached to a ready to use mouse, screen and keyboard?  Yes  No
- iii. Are administrator privileges well defined in your automation systems  Yes  No
- iv. Do you have change management guidelines for system configuration?  Yes  No
- v. Is there IT security training and awareness program /policy for employees?  Yes  No

#### (II)

- a) a) Is there functional IT security policy in the university? Yes  No
- b) What are the IT security standards / frameworks employed within the university?
  - a.  ISO 27001  ISO 27002  COBIT 27002
  - b.  Any other.....
- c) Is penetration testing conducted regularly for systems?  Yes  No
- d) Are there offices that do not access internet / network services?  Yes  No

- e) What are the total internet bandwidth levels in the university?
  - a. Below 30 Mbps  31-60 Mbps  61-100 Mbps  Over 100 Mbps
- f) Indicate the availability of the following in your IT network infrastructure;
  - i. Firewalls  Yes  No
  - ii. Intruder detection / prevention systems  Yes  No
  - iii. Honey pots and de-militarized zones  Yes  No
  - iv. User-groups  Yes  No
  - v. Unified threat management like cyberoam / mikrotik  Yes  No
  - vi. System controlled password expiry  Yes  No

**(III)**

- i. Is there system and data classification criterion for security purposes?  Yes  No
- ii. Are there ways of preventing data leak (un-authorized exposure of data) in the university?  Yes  No
- iii. Do you have automated regular off-site systems back-up for ERP  Yes  No
- iv. Does the ERP systems vendor still share the systems administrative rights?  Yes  No
- v. Can the ERP vendor access your systems remotely?  Yes  No
- vi. Given a second chance, would you accept the current ERP system again?  Yes  No

**(IV)**

Indicate the type of authentication that you use to access server room and resources?

- i. Biometrics:  Yes  No.
- ii. Access control cards:  Yes  No.
- iii. Any combination with password:  Yes  No
- iv. Any other.....

**(V)**

- i. Is there a recurrent budget to maintain IT security in the university? Yes  No
- ii. Do you have ways of measuring the returns on IT security investment?  Yes  No.  
If Yes, state the method.....
- iii. Have you ever experienced any IT security incidents within the university?
  - a. Yes  No  If yes, cite the incident.....
- iv. How can you rate the IT security levels in your university?
  - a. Secure  Insecure  Not sure .

**PART C: Information on relationship between IT Security Elements and Metrics**

- (a) Are there ways of measuring IT security status / levels in the university?  
Yes  No : If yes, state the ways.....

(b) Based on your opinion, you are requested to indicate the extent to which the listed sub-elements of the major elements of IT security influence the status (metrics) of IT security in the university. The major elements of IT being: *IT security Policy, Physical security, Network Security, data security and Access Control.*

For the tables below, please rate your response in a scale of 1 – 5, where, 1 = (Very ineffective), 2 = Ineffective), 3 = (Moderately Effective), 4 = (Effective), 5 = (Very Effective).

22	<b>Element one:</b>	<b>IT security Policy</b>				
	<b>Scales</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
		<b>Scale</b>				
	Policy is implemented and staff sensitized about it?					
	Policy meets the industry standards' requirements?					
	Policy specifies the consequences for violation?					
	Policy establishes the rules that guide behavior of users?					

23	<b>The Element two:</b>	<b>Physical security</b>				<b>Scale</b>					
	<b>Scales</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>					
		Implementation of Signage / mark posts along IT data lines?									
		Implementations of physical barriers around IT systems assets?									
		Implementation, adoption and maintenance of IT asset register?									
	Access control to physical facilities hosting IT systems?										
	Secure storage and monitoring of facilities e.g. through CCTV?										

24	<b>Element</b>	<b>Three: Network Security</b>				<b>Scale</b>					
	<b>Scales</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>					
		Network is hierarchical and managed?									
		Network is secured with virtual segmentations e.g. VLANs?									
		Conducting penetration testing against network security appliances?									
		Availability of internet bandwidth management tools?									
	Availability of alternative internet service provider (ISP) is used?										
	Redundant back-bones are used in the LAN?										

25	<b>The Element four: data security</b>	<b>Scale</b>				
		<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
		Successful data backup?				
		Successful data restoration?				
		Availability of critical servers and applications?				
	Malware control for data protection?					
	Encryption of electronic files in databases?					

26	<b><i>Element Four: Access Control</i></b>	<b><i>Scale</i></b>				
		<b><i>1</i></b>	<b><i>2</i></b>	<b><i>3</i></b>	<b><i>4</i></b>	<b><i>5</i></b>
	Control of access from external networks?					
	Penetration testing for security appliances?					
	Regular web content filtration?					
	Control of access from internal networks?					
	Control of access from external networks?					

### Appendix 3: Interview schedule.

#### The interview schedule

Interview Reference Number:

#### Theme: the relationship between IT Security Elements and Metrics

Note to Interviewer: *Instructions to you are in italics and enclosed in brackets. Questions for you to read out are in normal print*

*(Read out the following :)*

We are carrying out a research to investigate the major elements of focus in the management of IT security within universities in Kenya, and the elements' relationship with IT security metrics, in order to apply the elements in developing a suitable IT security metrics' model for the universities. Would you mind responding to a few questions on your experience with regards to this? *(If they decline, discontinue the interview and thank them.)*

*(Continue reading)*

Further, I wish to commence by assuring you that your answers will be treated with utmost confidentiality, that the information will be used solely to investigate the relationship between the elements and IT security metrics, and in the development of the suitable model. Further, all responses will remain anonymous.

1. (a) Do you have ways of measuring IT security status / levels in the university?  
Yes [ ] No [ ]: *(If "yes", tick and move to 1(b), if "No" skip it.)*  
(b) State the ways of measuring IT security status *(record as they are stated)*  
(c) How do you determine the returns on IT security investment?
2. Based on your opinion, kindly indicate the extent to which the listed sub-elements of the major elements of IT security influence the status (metrics) of IT security in the

university. The major elements of IT being: IT security Policy, Physical security, Network Security, data security and Access Control. Please rate your response in a scale of 1 – 5, where, 1 = (Very ineffective), 2 = Ineffective), 3 = (Moderately Effective), 4 = (Effective), 5 = (Very Effective).

(Read out the sub-elements under each major element and tick the corresponding appropriate scale)

<b>I</b>	<b>Element one: IT security Policy</b>					
		<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>
		<i>Scale</i>				
	Policy is implemented and staff sensitized about it?					
	Policy meets the industry standards' requirements?					
	Policy specifies the consequences for violation?					
	Policy establishes the rules that guide behavior of users?					

<b>II</b>	<b>The Element two: Physical security</b>	<i>Scale</i>				
	<i>Scales</i>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
	Implementation of Signage / mark posts along IT data lines?					
	Implementations of physical barriers around IT systems assets?					
	Implementation, adoption and maintenance of IT asset register?					
	Access control to physical facilities hosting IT systems?					
	Secure storage and monitoring of facilities e.g. through CCTV?					

<b>III</b>	<b>Element Three: Network Security</b>	<i>Scale</i>				
	<i>Scales</i>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
	Network is hierarchical and managed?					
	Network is secured with virtual segmentations e.g. VLANs?					
	Conducting penetration testing against network security appliances?					
	Availability of internet bandwidth management tools?					
	Availability of alternative internet service provider (ISP) is used?					
Redundant back-bones are used in the LAN?						

<b>IV</b>	<b>The Element four: data security</b>	<i>Scale</i>				
		<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>
	Successful data backup?					
	Successful data restoration?					
	Availability of critical servers and applications?					
	Malware control for data protection?					
Encryption of electronic files in databases?						

<b>V</b>	<b>Element Four: Access Control</b>	<i>Scale</i>				
----------	-------------------------------------	--------------	--	--	--	--

	<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>
Control of access from external networks?					
Penetration testing for security appliances?					
Conduct web content filtration?					
Control of access from internal networks?					
Control of access from external networks?					

3. Are there any ways you feel IT security metrics could be improved?  
*(Note down the various ways if stated)*

**Thank you very much for your time and responses.**

## Appendix 5: Program Code for the prototype

```
<html>
<?php
session_start();
$_SESSION['policy'];
$_SESSION['physical'];
$_SESSION['network'];
$_SESSION['access'];
$_SESSION['data'];

$policy=$_SESSION['policy'];
$physical=$_SESSION['physical'];
$network=$_SESSION['network'];
$access=$_SESSION['access'];
$data=$_SESSION['data'];
$q6=(1.9
+((1.6*$policy)/100)+((0.8*$physical)/100)+((0.8*$network)/100)+((0.8*$ac
cess)/100));
?>
<style type="text/css">
<!--
.style1 {
    font-family: Verdana, Arial, Helvetica, sans-serif;
    font-weight: bold;
}
.style3 {
    font-family: Georgia, "Times New Roman", Times, serif;
    font-weight: bold;
    font-size: 14px;
    color: #006633;
}
-->
</style>

<head>
<title></title>

</head>
<body>

<div style="width:800px;height:800px;-webkit-border-radius: 20px;-moz-border-radius:
20px;border-radius: 20px;background-color:#FFFFFF;-webkit-box-shadow: #76B36F 2px 2px
2px;-moz-box-shadow: #76B36F 2px 2px 2px; box-shadow: #76B36F 2px 2px 2px; margin-
right: auto; margin-left: auto; border:1px solid #033803; padding: 20px; ">
<div align="center">
    <p><span class="style1">Summary of scores per item:</span>
```

```

    <!-- Styles -->
    </p>
    <p>
    <style>
#chartdiv {
    width : 100%;
    height : 400px;
}

    </style>

    <!-- Resources -->
    <script src="https://www.amcharts.com/lib/3/amcharts.js"></script>
    <script src="https://www.amcharts.com/lib/3/gauge.js"></script>
    <script src="https://www.amcharts.com/lib/3/plugins/export/export.min.js"></script>
    </p>
</div>

<!-- Styles -->
<style>
#chartdiv1 {
    width          : 100%;
    height         : 200px;
    font-size      : 11px;
}
</style>
<!-- Resources -->
<script src="https://www.amcharts.com/lib/3/amcharts.js"></script>
<script src="https://www.amcharts.com/lib/3/serial.js"></script>
<script src="https://www.amcharts.com/lib/3/plugins/export/export.min.js"></script>
<link rel="stylesheet" href="https://www.amcharts.com/lib/3/plugins/export/export.css"
type="text/css" media="all" />
<script src="https://www.amcharts.com/lib/3/themes/light.js"></script>

<!-- Chart code -->
<script>
var chart = AmCharts.makeChart( "chartdiv1", {
    "type": "serial",
    "theme": "light",
    "dataProvider": [ {
        "area": "Policy",
        "values": <?php echo $policy; ?>
    }, {
        "area": "Physical",
        "values": <?php echo $physical; ?>
    }, {

```

```

    "area": "Network",
    "values": <?php echo $network; ?>
  }, {
    "area": "Access",
    "values": <?php echo $access; ?>
  }, {
    "area": "Data",
    "values": <?php echo $data; ?>
  }, {
    "area": " ",
    "values": 0
  } ],
  "valueAxes": [ {
    "gridColor": "#FFFFFF",
    "gridAlpha": 0.2,
    "dashLength": 0
  } ],
  "gridAboveGraphs": true,
  "startDuration": 1,
  "graphs": [ {
    "balloonText": "[[category]]: <b>[[value]]</b>",
    "fillAlphas": 0.8,
    "lineAlpha": 0.2,
    "type": "column",
    "valueField": "values"
  } ],
  "chartCursor": {
    "categoryBalloonEnabled": false,
    "cursorAlpha": 0,
    "zoomable": false
  },
  "categoryField": "area",
  "categoryAxis": {
    "gridPosition": "start",
    "gridAlpha": 0,
    "tickPosition": "start",
    "tickLength": 20
  },
  "export": {
    "enabled": true
  }
} );
</script>
<table width=100%>
<tr>

```

```

<td width="80%">
<!-- HTML -->
<div id="chartdiv1"></div>
  <link rel="stylesheet" href="https://www.amcharts.com/lib/3/plugins/export/export.css"
type="text/css" media="all" />
  <div align="center">
    <p>
      <script src="https://www.amcharts.com/lib/3/themes/light.js"></script>

      <!-- Chart code -->
      <script>
var gaugeChart = AmCharts.makeChart( "chartdiv", {
  "type": "gauge",
  "theme": "light",
  "axes": [ {
    "axisThickness": 2,
    "axisAlpha": 0.2,
    "tickAlpha": 0.2,
    "valueInterval": 0.5,
    "bands": [ {
      "color": "#cc4748",
      "endValue": 4.1,
      "startValue": 1.9
    }, {
      "color": "#fdd400",
      "endValue": 6.1,
      "startValue": 4.1
    }, {
      "color": "#228B22",
      "endValue": 7.1,
      "innerRadius": "95%",
      "startValue": 6.1
    } ],
    "bottomText": "0",
    "bottomTextYOffset": -0.5,
    "endValue": 7.0
  } ],
  "arrows": [ {} ],
  "export": {
    "enabled": true
  }
} );

setInterval( randomValue, 2000 );
// set random value
function randomValue() {

```

```

var value = <?php echo $q6; ?>;
if ( gaugeChart ) {
  if ( gaugeChart.arrows ) {
    if ( gaugeChart.arrows[ 0 ] ) {
      if ( gaugeChart.arrows[ 0 ].setValue ) {
        gaugeChart.arrows[ 0 ].setValue( value );
        gaugeChart.axes[ 0 ].setBottomText( value + " " );
      }
    }
  }
}
}
}
}
</script>
</p>
<p><span class="style1">Overall analysis of results </span>
</p>
</div>
<div id="chartdiv"></div>
<p>The score on the overall security is:<span class="style3"> <?php echo $q6; ?> </span></p>
<p align="right"><a href="m.php"></a></p>
</div>
</td>
<td width="20%">
<table>
<tr>
<td colspan="2"> KEY</td>
</tr>
<tr bgcolor="red">
<td>1.9-4.0</td>
<td>Severe security</td>
</tr>
<tr bgcolor="yellow">
<td>4.1-6.0</td>
<td>Insecure</td>
</tr>
<tr bgcolor="green">
<td>Above 6.0</td>
<td>Safe</td>
</tr>
</table>
</td>
</tr>
</table>
</body>
</html>

```

**Appendix 6: List of the universities, source CUE 2015**