EXAMINING INFORMATION SECURITY CONTROLS IN THE HUMAN RESOURCE DEPARTMENT OF KAMPALA INTERNATIONAL UNIVERSITY, UGANDA FROM 2013-2018

BY:

MBABAZI STELLA

MIS/39650/131/DU

A Thesis

Presented to the

College of Higher Degrees and Research

Kampala International University

Kampala, Uganda

_____

In Partial Fulfillment of the Requirements for the Degree

Of Masters of Science in Information Systems

November 2018

DECLARATION

I declare that this thesis is my original work and to the best of my knowledge it has never been submitted before for academic purpose or published by any institution of higher learning.

Signature: ……..

Date: ……

Name: MBABAZI STELLA

Researcher

APPROVAL

"I confirm that the work reported in this thesis was carried out by the researcher under my supervision."

Signature Date

……..... ……..

Dr. Kareyo Margaret

Supervisor

DEDICATION

This work is dedicated to my Lovely Husband, Children, Mother and friends for all the love, support and time they gave me.

ACKNOWLEDGEMENT

The completion of this work was due to the support rendered to me by many people to whom I owe acknowledgement. First and foremost I thank the Almighty God for the protection and courage he gave me towards the completion of this thesis and the entire programme. In a special way, am thankful to my beloved husband, children, and mother for their support.

I wish to acknowledge the invaluable support rendered by the staff of Kampala International University towards the success of my thesis and also during my entire period of study.

I am greatly indebted to my supervisor Dr. Kareyo Margaret for the scholarly advice, support and guidance she offered me to ensure that I get this far. My thanks also go to Dr. Norah Naiboka and Dr. Malinga for their scholarly advice and guidance.

My sincere thanks also go to my relatives and friends who offered me encouragement and also stood by me in all my endeavors.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

ANOVA	Analysis of variance
CCTV	Closed-circuit television
CIA	Confidentiality, Integrity, Availability
CIO	Chief Information Officer
CoHSS	College of Humanities and Social Science
CSI	Computer Security Institute
CVI	Content Validity Index
DECs	Department Examination Co-coordinators
DDoS	Distributed Denial-of-Service
DMZ	Demilitarized Zone
E-government	Electronic government
E-security	Electronic security
FBI	Federal Bureau of Investigation
FFIEC	Federal Financial Institutions Examination Council
HR	Human Resource
IA	Information Assurance
ICT	Information and communication technology
IT	Information Technology
IDS	Intrusion Detection Systems
ISC	Information Security Culture
ISMS	Information Security Management System
ISO	International Standard Organization
IRB	Institution Review Board

JNSA	Japan Network Security Association
KIU	Kampala International University
MoICT	Ministry of Information and Communications Technology
NHS	National Health Service
NSSF	National Social Security Fund
OECD	Organization for Economic Co-operation and Development
PIN	Personal Identification Number
PKIs	Public Key Infrastructures
PLCC	Pearson Linear Correlation Co-efficiency
PwC	Price Waterhouse Coopers
POPI	Protection of Personal Information Bill
QA	Quality Assurance
SCIT	School of Computing and Information Technology
SD	Standard Deviation
SEAS	School of Engineering and Applies Science
SMTP	Simple Mail Transfer Protocol
SoL	School of Law
SPSS	Statistical Package for Social Scientists
TLCs	Teaching and Learning Coordinators

ABSTRACT

The research study was based on examining information security controls in the Human Resource Department of KIU, Uganda. The objectives of the study were; to analyze the information security controls in the Human Resource department of Kampala International University, to explore the extent of compliance to information security objectives at Kampala International University, to investigate the challenges of information security at Kampala International University, and also to ascertain if there was a significant relationship between challenges of information security of records and security objectives at Kampala International University. A correlation study was used to establish if there was a significant relationship between challenges of information security and security objectives at Kampala International University. This was because the study focused on establishing if there was a significant relationship between challenges of information security and security objectives in Kampala International University. A sample size of 65 respondents was taken from the target population of 78 respondents using the solvens formula; data was analyzed using Statistical Package for Social Scientists (SPSS) version 16.0. Pearson Linear Correlation Co-efficiency (PLCC) was used to establish if there is a significant relationship between challenges of information security and security objectives at KIU. The study found out that there was no significant relationship between challenges of information security of records and security objectives in KIU. The level of significance was 0.460 which implied that there was no significant relationship between challenges of information security and security objectives in KIU. The null hypothesis was accepted and the alternate hypothesis was rejected. This therefore caused the researcher to suggest the following recommendations: KIU; should ensure that information is not disclosed to unauthorized persons by ensuring that there is tight security in information based areas, should protect information from being modified by unauthorized parties by ensuring password usage, should maintain an ongoing awareness of attack threats through security information sources, should educate its employees in safe computing practices, such as installing anti-virus software on servers and desktops.

CHAPTER ONE

INTRODUCTION

1.0 Background of the study

Information and records are valuable resources in any organization and as such, there is need for establishing security measures to safe guard them for instance many organizations need to process and keep information for effective management; universities keep staff bio-data, payrolls, students transcripts and many others, hospitals maintain patients' records to monitor their clients' health changes and Internet service providers log traffic for research purposes and to identify unauthorized activity, customers also recognize the need for obtaining and processing this data into useful information, but expect a certain degree of confidentiality in order to protect their privacy (Vigo, 2011).

Vigo (2011), further states that developing policies such as keeping information in locked storage areas, equipping computers with access codes or passwords that are changed periodically, encrypting data that is sent or received electronically and installing firewalls, and limiting information access to unauthorized people, are important for keeping information confidential.

Globally, information security and confidentiality is a very important aspect in the management of records. A research carried out in Japan, according to the Survey Report of Information Security Incidents released every year by the Japan Network Security Association (JNSA), 1,032 security incidents had happened, theft and loss resulting from individual human error accounted for 42 per cent of all incidents and was the largest category (JNSA, 2010). In response to these types of situations, many products aimed at preventing information leaks became available in the market and management practices, such as Information security management system (ISMS), had been implemented. However, in the 2009 survey, information leakage incidents had failed to decline, with the number reaching 1,539 incidents. Although individual human error incidents had declined to 7.9% per cent, incidents caused by administrative error had increased from 5.1% per cent in 2005 to 50.9% per cent. Based on these statistics, new approaches for information security measures had risen (Komatsu et al., 2013).

Information security at a university setting is a "*negative deliverable*", this means that when strong security policies are in place, security remains generally unnoticed, but when it is absent, it is very noticeable, for these reasons higher education has difficult providing resources for information security (Schiller, 2002). Schiller (2002), also states that many university users do

not understand very basic information security threats, for example, how a compromised system can be used to attack another system on the Internet or why password protection can lead to identity theft.

Academic institutions face unique information security threats as well as increasingly frequent and severe incidents, yet they have invested relatively few resources to define and address these issues. Incidents such as information theft, data tampering, viruses, worms, and terrorist activity constitute significant threats to the security of academic institutions (Burd, 2005).

The bond of confidentiality between a patient and those providing treatment is a basic tenet of the National Health Service (NHS). It ensures that confidential clinical data are used in the most effective and secure way to deliver the best treatment, and that the patient's trust is retained (Keyser, 2004).

In Africa, for example South Africa, information about a person's health and health care is generally considered to be highly sensitive and personal, therefore deserving of the strongest protection under the law (Gill, 2012). Gill (2012), further notes that South African healthcare legislation and codes of conduct do account for this protection but that the Protection of Personal Information Bill, (POPI Bill) has a significant impact on data privacy, including in respect of personal healthcare information when it is promulgated.

In a bid to look at records in Africa and Uganda in particular, emphasis was put at: inadequate finding aids **(**tools that help a user find information in a specific record group, collection, or series of archival materials); lack of recognition by national governments of the role played by records centers; inadequate number of professional records managers; lack of adequate records training schools; poor systems of records arrangement and description; understaffing of records services; poor storage facilities for records; and inadequate retrieval tools (Mnjama, 2005).

In Uganda, When the Uganda Radio Network visited the Records Department at Mulago hospital in the year 2006, the department had no computerized record system, the department was also still operating an outdated manual records keeping system and this therefore was affecting the security and confidentiality of patients' information, the Uganda Radio Network found when there were hundreds of medical files, correspondence, hospitalization summaries, patient labels and reports which were heaped all over the floor of a small cramped office, it was also reported that the most affected areas by the lack of space were the obstetrics and gynecology departments, whose files were found lying in the corridors, waiting to be collected by cleaning companies and eventual destruction (Odongtho, 2006).

Due to lack of basic records management knowledge or limited interest in information management within Bank of Uganda (BoU), many information seekers lack the most suitable way of seeking for information to satisfy their needs and therefore end up failing to formally state exactly what they need, this eventually leads to low satisfaction on the users' side and also inefficiency on the service provider's performance (Lutaaya, 2015).

Limited knowledge and awareness about proper records management procedures as a major business unit is still lacking in most government departments, this leads to poor records management practices like misfiling and improper indexing (Lutaaya, 2015).

There were security issues within National Social Security Fund (NSSF) where the Managing Director brought from Price Waterhouse Coopers (PWC) as an expert on pensions was kicked out at the heat of the Temagalo scandal. Chimpreports also established that one senior partner at PwC, was battling NSSF in court after the fund accused him of forgery and uttering false documents that saw him have access through the Fund's land in Lubowa.

Kampala International University is a private university which has built a name in Uganda's education sector with remarkable resilience and its Mission is to respond to societal needs by designing and delivery of an education guided by the principles and values of respect for society, economy and environment and to provide and develop a supportive research environment in which scholars at every stage of their career can flourish. The information security techniques used at KIU include; physical security (use of security guards, fence and locks), use of closed-circuit television camera (CCTV) in one of the departments (library), and use of passwords. Despite the fact that the University has some security techniques, there have been some information security issues such as; examination malpractice, and cases of students missing results.

1.1 Statement of the problem

In today's world of digital information, mobile business, interconnectivity and remote work places, there is one word that must be top of mind for any organization: security especially when employees and proprietary business data begin to mix; that is why over the years, Kampala International University Human Resource department has had issues related to information security for instance; payroll management, benefits and others. This puts a question on the mode of information security controls in KIU.

Due to the sensitivity of the subject, the researcher decided to study information security controls in KIU focusing on the Human Resource section (HR) which was deemed not to be so sensitive.

The study focused on administrative staff because they are the major information users and custodians.

Majority of the world's leading global organizations across all industries are constantly challenged in successfully achieving their strategic and tactical business and technology objectives in an effort to provide true-value to their stakeholders as a result of insufficient information security measures (Garbars, 2002).

Information security has been regularly considered to be a technological problem with a technological solution, which is simply untrue because information security is about managing risk (Whitman, 2005). Managing risk is about discovering and measuring threats to information assets in the organization and taking actions to respond to those threats (Lampson, 2002). Many university users do not understand very basic security threats, for example, how a compromised system can be used to attack another system on the Internet or why password protection can lead to identity theft (Schiller, 2002). .

1.2 General objective

The study aimed at examining information security controls in the Human Resource department of Kampala International University, Uganda.

1.3 The specific objectives were:

i. To examine information security controls in the HR section of KIU.
ii. To explore the extent of compliance to information security objectives at KIU.
iii. To investigate the challenges to information security at KIU.
iv. To ascertain if there was a significant relationship between information security objectives and challenges to information security of records at KIU?

v. 1.4 Research questions

i. What are the information security controls in the HR section of KIU?
ii. What is the extent of compliance to information security objectives at KIU?
iii. What are the challenges to information security of records at KIU?
iv. Is there a significant relationship between information security objectives and challenges to information security of records at KIU?

1.5 Hypotheses

i. **H_1:** There is a significant relationship between information security objectives and challenges to information security at KIU.
ii. **Ho:** There is no significant relationship between information security objectives and challenges to information security of records at KIU.

1.6 Scope

1.6.1 Conceptual scope

Information security relates to an array of actions designed to protect information and information systems" (Gordon & Loeb, 2006, p.121). However, information security does not cover only the information itself but also the entire infrastructure that facilitates its use. It covers hardware, software, threats, physical security and human factors, where each of these components has it is own characteristics. Given that the number of organization security breaches is increasing daily, and the more accessible the information, the greater the hazards, it is inevitable that security will need to be tightened (Brown & Duguid, 2002). The study focused on examining information security controls in the Human Resource Department (HRD) of KIU, Uganda. Due to the sensitivity of information, the researcher chose to do the research in a less sensitive Human resource department. It was the study in the HRD that could reveal some information of what was taking place in other departments. The researcher discovered that at KIU there was an academic policy, ICT policy, Human Resource policy but there was no an information security policy.

1.6.2 Geographical scope

The study was conducted from within the following departments (admissions, library, records, marketing, quality assurance and Information communication technology (ICT)), schools (School of Computing and Information Technology (SCIT), School of Law (SoL), School of Engineering and applied science (SEAS)) and colleges (College of humanities and social sciences (CoHSS)) at Kampala International University (KIU), main campus, Kampala – Uganda. The administrative staff was the targeted respondents because they are the ones who work with information concerning the university.

1.6.3 Theoretical scope

According to Schuessler (2009), General Deterrence Theory states that individuals can be dissuaded from committing antisocial acts through the use of countermeasures which include strong disincentives and sanctions relative to the act. Schuessler (2009) also noted "Using General Deterrence Theory as a guideline, countermeasures could be put in place to eliminate such a threat or at least mitigate some of the risk should the event occur, in this way other threats such as natural disasters and technical failures can also be examined.

1.6.4 Time scope

The research was conducted from January 2013 to February 2018.

1.7 Significance of the study

The study will help KIU staff know the appropriate measures to use so as to safe guard the security of the University's records. The study will help future researchers during their research studies. The study will improve awareness about information security of records, the information security objectives and also challenges to information security. The outcomes of the study will also be relevant to the institution to develop and deploy sound information security measures that will effectively protect its information assets.

1.8 Operational definition of key terms as used in this work

In context of this study;

Information refers to clusters of facts that are meaningful and useful to human beings in processes such as making decisions.

Information security controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information computer systems or other assets.

Record refers to a thing constituting a piece of evidence about the past, especially an account of an event or occurrence kept in writing or some other permanent form or device.

CHAPTER TWO

LITERATURE REVIEW

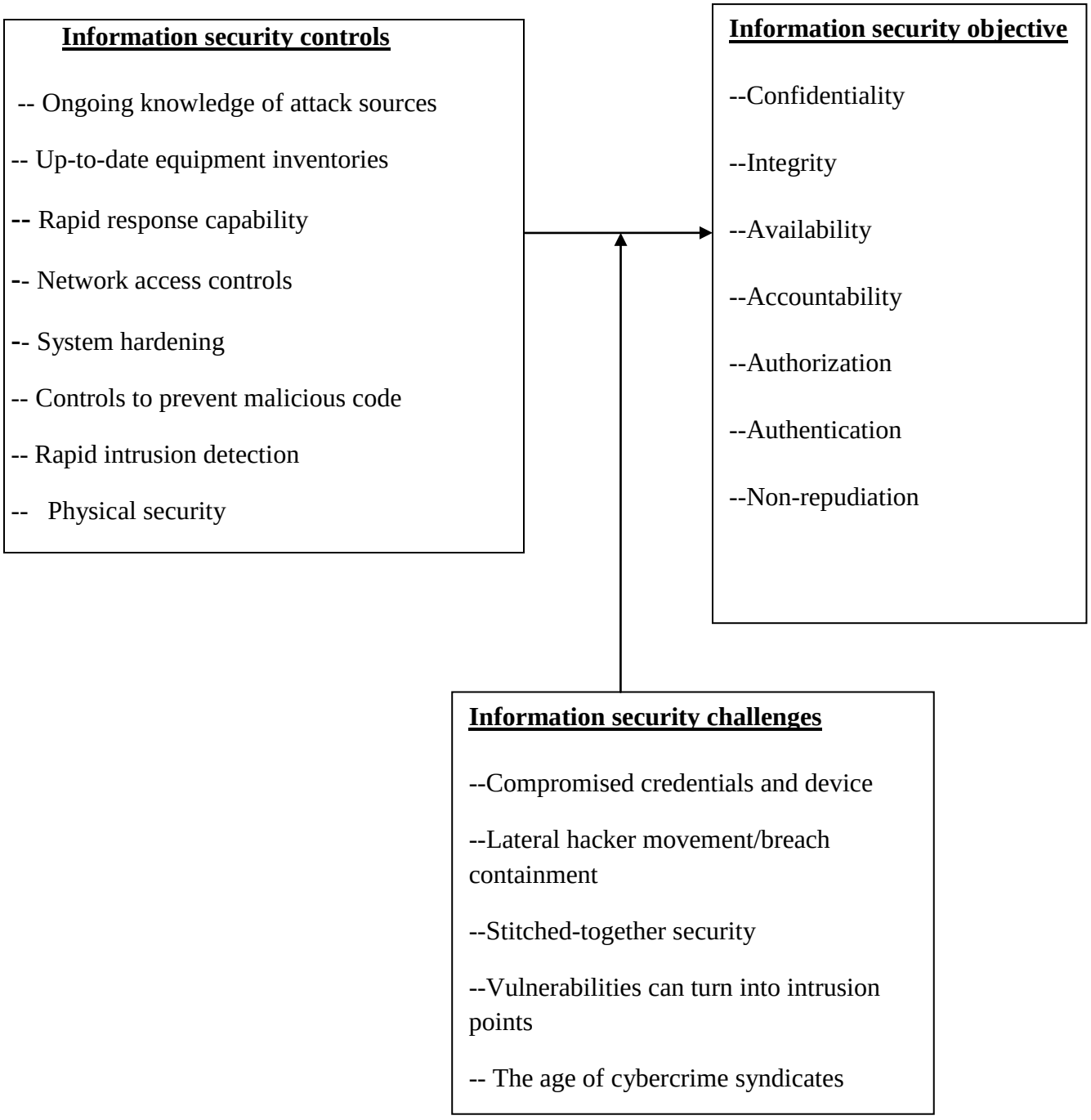
2.0 Introduction

This chapter consists of the theory, conceptual framework, and literature on: information security, Human resource in the context of information security, information security objectives, information security controls, information security challenges, related studies and research gap.

2.1 Theoretical review

According to Schuessler (2009), General Deterrence Theory states that individuals can be dissuaded from committing antisocial acts through the use of countermeasures which include strong disincentives and sanctions relative to the act. Schuessler (2009) also noted that using General Deterrence Theory as a guideline, countermeasures could be put in place to eliminate a threat or at least mitigate some of the risk should the event occur, in this way other threats such as natural disasters and technical failures can also be examined. The General deterrence theory suggests that when the possibility of punishment is high and the sanction is severe, potential criminals will be deterred from committing illegal acts, especially when their motives are weak (Theoharidou, 2005). Deterrent controls are designed to discourage individuals from intentionally violating information security policies or procedures; they usually take the form of constraints that make it difficult or undesirable to perform unauthorized activities or threats of consequences that influence a potential intruder to violate security, for example threats ranging from embarrassment to severe punishment (Tipton, 2007).

2.2 Conceptual framework



Conceptual Framework for examining information security controls, security objectives and security challenges at Kampala International University.

The conceptual framework was adapted from (Schuessler, 2009; Tipton, 2007; Spafford, 2007). According to Schuessler (2009), General deterrence theory states that individuals can be dissuaded from committing antisocial acts through the use of countermeasures which include strong disincentives and sanctions relative to the act. Schuessler (2009) also noted "Using General Deterrence Theory as a guideline, countermeasures could be put in place to eliminate such a threat or at least mitigate some of the risk should the event occur, in this way other threats such as natural disasters and technical failures can also be examined.

According to Tipton (2007), deterrent controls are designed to discourage individuals from intentionally violating information security policies or procedures; they usually take the form of constraints that make it difficult or undesirable to perform unauthorized activities or threats of consequences that influence a potential intruder to violate security, for example threats ranging from embarrassment to severe punishment.

Some information security challenges are caused by information security controls within a given organization, if the information security controls are weak or non-existent information security challenges are more likely to occur (Spafford, 2007). The amount of protection required depends on how likely a security risk is to occur and how big an impact it would have if it did occur, protection is achieved by a combination of technical and non-technical safeguards; for example for large enterprises there is a major task with a layered series of safeguards such as physical security measures, organizational measures, security procedures, background checks, user identifiers, passwords, smart cards, biometrics and firewalls (Spafford, 2007).

According to Lampson (2002), an organization's systems still remain vulnerable to attack after thirty years of accumulated work on security, the reason is probably that security setup is costly and difficult to sustain.

So generally speaking, as reflected in the conceptual framework, it’s hypothesized that compliance or achievement of total information security objectives is directly affected by the information security controls put in place. Nevertheless, that relationship is subject to the influence of any existing challenges.

2.2.1 Information Security Culture model

In determining what attributes to examine in relation to information security culture, the present study suggests a number of specific attributes that can be proposed:

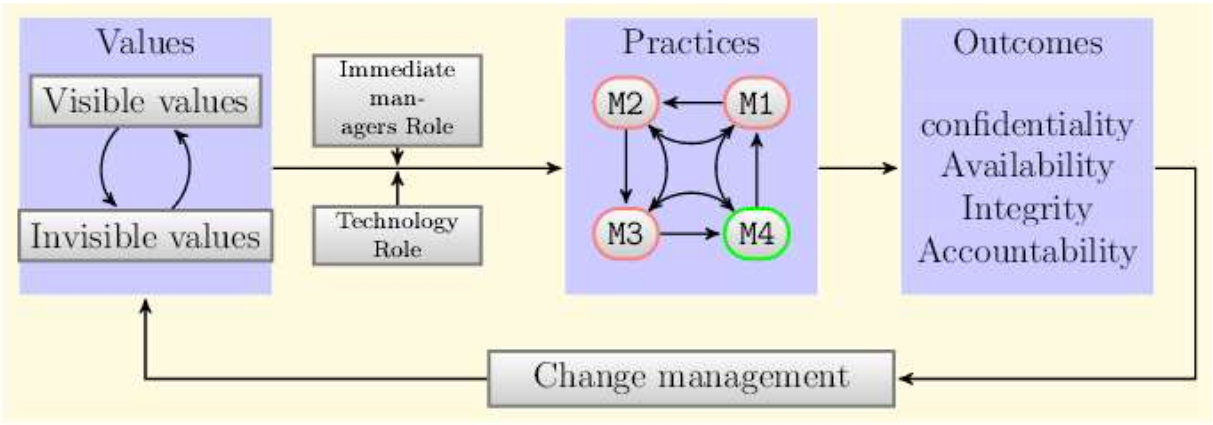


Figure 2.2.1: Information Security Culture model

The first two attributes can be viewed as corresponding to Schein (2004)'s three levels model:

Visible activities: The visible manifestations may include any activities which organizations can perform to either optimize their information security culture or adapt them to emphasize and achieve information security culture through appropriate management and employee behaviours. They may include any physical environment and management related activities such as commitment of top management, security related standards, policies, procedures, training and awareness programs on information security related attitudes and behaviour for members of specific organizations.

Invisible values: They capture the assumptions, attitudes, beliefs, values, and norms related to members of specific organizations in a given country. They are conceptualized by the organizational culture and national cultural values, which are believed to have influence on the information security related behaviours of an organization's employees.

Information security practices: Information security practices relate to the actual security related behavior of an organization's employees that appears to be influenced by values and activities relevant to the technological, organizational and national cultural aspects.

Outcomes: The outcomes that serve as a desired output to protect the information properties of confidentiality, integrity, availability and accountability.

Change management: This represents the relevant initiatives to emphasize or change the status quo to achieve information security culture through appropriate management and employee behaviors. As threats increasingly evolve and technology changes then the context within which an organization operates will become more vulnerable to various threats. The introduction of new technologies and business practices may lead to integrations and transformations between various aspects of information related values, assumptions and behavior.

Mediating factors: These relate to factors through which the influence of values is mediated. Immediate managers and supervisors have a great role to play. Real security culture lies in the security related beliefs, values, which manifest in employee's actions and behaviors towards information security problems. Therefore, organizations need to carefully think about the desired level of information security culture to influence their employees' behavior to protect organizational information.

2.3 Information security

This section looks at information security as discussed by the various authors, experts.

According to Von Solms (1996), information security has evolved through three stages: the first stage began in the 1960's when information security's major concern was to ensure and control physical security of the facilities; for example, printouts were circulated in protected ways. The second stage started in the mid-1970s when information security was tailored to the specific needs of individual organizations, despite the fact that the scope of information security had extended radically. In the third stage, with the advent of advanced technology, organizations needed to link their Information technology (IT) services together and move from a closed environment to complex environments that work in distributed and connected networks of machines. What makes information security very important nowadays in organizations is the type of environment people work in.

Organizations depend more and more on computers and computing control has been brought down to the individual desktop, more employees are interacting with technology to undertake their daily tasks, and employees constitute a greater threat because they have direct access to an organization's assets (Madigan, 2004). Information security is the process, by which an organization protects and secures its systems, media and facilities that maintain information vital to its operations with security, as an ongoing procedure and not a state at a point in time (FFIEC, 2006). This process of information security includes management of information security, network security, computer and data security (Bhatnagar & Sharma, 2012).

According to Lampson (2002), an organization's systems still remain vulnerable to attack after thirty years of accumulated work on security; the reason is probably that security setup is costly and difficult to sustain. There is a perception amongst employees that security gets in the way and that it interferes with employees' ability to accomplish tasks (Sandhu, 2003). Straub and Welke sum up the situation as follows: "Information security continues to be ignored by top managers, middle managers, and employees alike. The result of this neglect is that organizational systems are far less secure than they might otherwise be and that security breaches are far more frequent and damaging than is necessary" (Straub & Welke, 1998, p. 441). In order for organizations to achieve a stronger protection of their information the recognition of the main threats facing organizational information is urgently required (Whitman, 2003). Threats are "circumstances that have the potential to cause loss or harm" to information and can be classified as external and internal ((Pfleeger, 1997, p.3 & Hind, 2002).

According to Doherty & Fulford (2005), the sources and consequences of threats to information faced by organizations are quantified through the use of surveys, the following threats have been identified by these surveys: External threats; computer viruses, natural disaster, spam emails and hacking incidents. Internal threats: installation or use of unauthorized hardware, peripherals; abuse of computer access controls; physical theft of hardware or software; human mistake; damage by displeased employee; use of organization resources for illegal communications or activities (porn surfing, email harassment) and installation or use of unauthorized software.

Information security is the process, by which an organization protects and secures its systems, media and facilities that maintain information vital to its operations with security, as an ongoing procedure and not a state at a point in time (FFIEC, 2006). This process of information security includes management of information security, network security, computer and data security (Bhatnagar & Sharma, 2012). Information security is important as it plays a key role in the successful adoption of new technologies; it determines trust and security assurance for new technologies by the intended adopters and implementers (Conklin, 2007).

Security is an important problem in the spread of computer network technology (Zhou & Hu, 2008). Ensuring information security enables the security problem to be addressed. This is through implementation and meeting the information properties of confidentiality, integrity, and availability of records. Guaranteeing the above information properties strengthens user services such as authentication, authorization, accountability and reliability (Alfawaz *et al*., 2008). Information security therefore is vital in the achievement of information, network, computer and data security and in turn the success of e-government adoption.

According to Cherdantseva & Hilton (2013), information security refers to the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption however, according to Dore (2007), information security provides the management processes, technology and assurance to ensure business transactions can be trusted, information technological services are usable and can appropriately resist and recover from failure due to error, deliberate attacks or disaster and ensure critical confidential information is withheld from those who should not have access to it. On the other hand, information security's objective is to protect the interests of those relying on information and the systems and communications that deliver the information from harm that would result from failures of availability, confidentiality, and integrity (Spafford, 2007).

According to Spafford (2007), for most users the security objective is met when, information systems are available and usable when required, and can appropriately resist attacks and recover from failures (availability), information is accessed by or disclosed to only those who have a right to know (confidentiality), information is protected from unauthorized modification or error so that accuracy, completeness and validity are maintained (integrity), business transactions and exchanges between enterprises, customers, suppliers, partners and regulators can be trusted (authenticity and non-repudiation). The amount of protection required depends on how likely a security risk is to occur and how big an impact it would have if it did occur, protection is achieved by a combination of technical and non-technical safeguards. For example for large enterprises there is a major task with a layered series of safeguards such as physical security measures, organizational measures, security procedures, background checks, user identifiers, passwords, smart cards, biometrics and firewalls (Spafford, 2007).

According to Boritz (2011), information security has got three principles which include; confidentiality, integrity, availability (CIA). He further states that the CIA principles have to guide people about their perception of information security and that a security breach needs not to be a malicious act; it could be as innocent and simple as a power outage or a failure to set network access privileges correctly, or it could be the total loss of all your facilities through a disastrous event, natural or unnatural, well as according to Anderson (2001), in one of his common view, information security comes down to technical measures, that is given better access control policy models, formal proofs of crypto-graphic protocols, approved firewalls, better ways of detecting intrusions and malicious code, and better tools for system evaluation and assurance.

According to Demopoulos (2002), Information Security is simply the process of keeping information secure that is protecting its availability, integrity, and privacy. He further states that information security is a process while according to Schneider (2013), information security is protecting information and information systems from unauthorized access, use, disruption, or destruction. The terms information security, computer security and information assurance are frequently used interchangeably. She further states that institutions of all sizes collect and store huge volumes of confidential information, the information may be about employees, customers, research, products or financial operations, most of this information is collected, processed and stored on computers and transmitted across networks to other computers and if this information fell into the wrong hands, it could lead to business loss, law suits, identity theft or even bankruptcy of the business.

Computer security is security applied to computers, computer networks, and the data stored and transmitted over them, this field covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction (Moore, 2005).

According to Kabay (2004), the basic reasons we care about information systems security are that some of our information needs to be protected against unauthorized disclosure for legal and competitive reasons; all of the information we store and refer to must be protected against accidental or deliberate modification and must be available in a timely fashion, we must also establish and maintain the authenticity (correct attribution) of documents we create, send and receive. Finally, if poor security practices allow damage to our systems, we may be subject to criminal or civil legal proceedings; if our negligence allows third parties to be harmed via our compromised systems, there may be even more severe legal problems. Kabay (2004), further note that, in e-commerce good security can be seen as part of the market development strategy, consumers have expressed widespread concerns over privacy and the safety of their data; companies with strong security can leverage their investment to increase the pool of willing buyers and to increase their market share. There is no need to look at security purely as loss avoidance: in today's marketplace good security becomes a competitive advantage that can contribute directly to revenue figures and the bottom line.

2.3.1 Information assurance

According to Jacobs (2011), Information assurance (IA) is the practice of managing information-related risks, more specifically, IA practitioners seek to protect and defend information and information systems by ensuring confidentiality, integrity, authentication, availability, and non-

repudiation. These goals are relevant whether the information is in storage, processing, or transit, and whether threatened by malice or accident. In other words, IA is the process of ensuring that authorized users have access to authorized information at the authorized time however according to Schou (2007), in information assurance due care is characterized by a careful attention to detail in the process of designing, assessing, updating and monitoring data and systems. He further states that it has control implications as well. He also states that the assumption is that an ethical organization will always exercise due care in the enforcement of confidentiality and integrity requirements. According to Schou (2007), information assurance has a life cycle. He stated that properly functioning systems produce consistent outcomes and in order to achieve consistency, systems incorporate a common set of elements into a logical process. The information assurance life cycle is divided into four sections as follows (Schou, 2007).

Section one: Understanding the risks, the first section, composed of two chapters, outlines the two primary principles that are the stating place for the information assurance process. These are necessary because information is intangible. Therefore has to be an initial stage to identify and label the information that the organization owns and recognize what threatens it. The first chapter presents a process to ensure that all items of value to the organization are identified and accounted for. Without this process, the organization would not know what to secure. Once each information asset is identified and catalogued, a risk assessment is carried out to define the specific things that might harm each item. Specific knowledge of the risks is a precondition to establishing a correct response. This involves: Understanding the form of the asset and also assessing risks.

Section two: Sustaining a relevant response, to ensure trust, the information assurance process has to be sustainable. Sustainability requires a concrete and repeatable infrastructure of processes that are continuously appropriate and persistent. Section two discusses the principles that the organization must address to ensure a systematic response. This involves: Establishing an overall process, building and documenting an information assurance framework, maintaining security of operations, and controlling access.

Section three: Deploying the countermeasures, the countermeasures are the traditional areas of security. This section is composed of eight chapters, organized into management and technical countermeasures. All these areas are broad and deep and each contains more material than could possibly be presented in a single textbook because they represent substantive actions. Consequently concentration is put on discussing their general application and their interrelationship with each other. This entails: Management countermeasures which include;

Personal security, physical security, assuring against software vulnerability, continuity planning and implementation, laws, regulations and computer crimes. Technical countermeasures include; Network security, cryptology, and ensuring the secure use of software.

Section four: Sustaining a security culture, finally two aspects of the assurance process do not fit directly within a life cycle model. These are ethics and human factors. These are higher-level principles, which support the "security behavior" of the organization. Although they appear to be peripheral to establishing a security system, they are critical to its long-term success. This section includes; Human factors: Ensuring secure performance and ensuring an ethical organization.

2.3.2 Network security

Network security consists of the policies adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources (Wright & Jim, 2009). Wright & Jim (2009) further stated that Network security involves the authorization of access to data in a network, which is controlled by the network administrator; users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority.

On the other hand according to Schou (2007), network security protects electronic communication from unauthorized modification, destruction, or disclosure and ensures that an increasing number of diverse attacks do not harm the distributed critical information infrastructure. It is the range, diversity, and extent to those attacks and the complexity of the medium that makes securing a network a compelling and difficult task. He further notes that network security has a dual mission. First, it ensures the accuracy of the data transmitted. Second, it must also protect confidential information processed, stored on, and accessible from networks while ensuring the network is always available to authorized users.

2.3.3 Electronic security

According to Obaidat (2009), electronic security (e-security) is an important issue to businesses and governments today. He further states that e-security addresses the security of a company, locates its vulnerabilities, and supervises the mechanisms implemented to protect the on-line services provided by the company, in order to keep adversaries (hackers, malicious users, and intruders) from getting into the company's networks, computers, and services. Electronic security is an important aspect that needs to be considered while dealing with electronic transactions. For instance, according to Labuschagne (2000), the major reason why most people are still skeptical

about electronic commerce is the perceived security risks associated with electronic transactions over the Internet. The Internet, however, holds many opportunities that could mean survival or competitive advantage for many organizations. To exploit these opportunities, it is important to first analyze the risks they hold. Electronic commerce is based on business as well as technological risks, making it a very difficult environment to secure. Apart from these two types of risk categories there are several other issues and problems that need to be addressed.

On the other hand according to Glaessner (2002), electronic security can be described as those policies, guidelines, processes, and actions needed to enable electronic transactions to be carried out with a minimum risk of breach, intrusion, or theft. Glaessner (2002) states further that, electronic security is any tool, technique, or process used to protect a system's information assets. Information is a valuable strategic asset that must be managed and protected accordingly. The degree of electronic security used for any activity should be proportional to the activity's underlying value. Thus, security is a risk-management or risk-mitigation tool, and appropriate security means mitigation of the risk for the underlying transaction in proportion to its value. Glaessner (2002) further noted that the need for security is a constant of doing business over the Internet because, in essence, the Internet is a broadcast medium. Electronic security enhances or adds value to a naked network and is composed of both a "soft" and a "hard" infrastructure. Soft infrastructure components are those policies, processes, protocols, and guidelines that create the protective environment to keep the system and the data from compromise. The hard infrastructure consists of the actual hardware and software needed to protect the system and its data from external and internal threats to security.

2.3.4 Information security threats

According to Wright & Jim (2009), in computer security a threat is a possible danger that might exploit a vulnerability to breach security and thus cause possible harm. However Cherdantseva & Hilton (2013) point out that computer system threats come in many different forms. Some of the most common threats today are software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion. Most people have experienced software attacks of some sort. Viruses, worms, phishing attacks, and Trojan horses are a few common examples of software attacks.

Virus: Attackers can develop harmful code known as viruses. Viruses in general are a threat to any environment. They come in different forms and although not always malicious, they always take up time. Viruses can also be spread via e-mail and disks.

Trojan horse: These are malicious programs or software code hidden inside what looks like a normal program. When a user runs the normal program, the hidden code runs as well. It can then start deleting files and causing other damage to the computer. Trojan horses are normally spread by e-mail attachments.

Worms: These are programs that run independently and travel from computer to computer across network connections. Worms may have portions of themselves running on many different computers. Worms do not change other programs, although they may carry other code that does.

Password cracking: This is a technique attackers use to surreptitiously gain system access through another user's account. This is possible because users often select weak passwords.

Denial-of-service attacks: This attack exploits the need to have a service available. It is a growing trend on the Internet because Web sites in general are open doors ready for abuse.

E-mail hacking: Electronic mail is one of the most popular features of the Internet. With access to Internet e-mail, someone can potentially correspond with any one of millions of people worldwide.

2.3.5 Some of the threats associated with e-mail are:

Impersonation: The sender address on Internet e-mail cannot be trusted because the sender can create a false return address. Someone could have modified the header in transit, or the sender could have connected directly to the Simple Mail Transfer Protocol (SMTP) port on the target computer to enter the e-mail.

Packet replay: This refers to the recording and retransmission of message packets in the network. Packet replay is a significant threat for programs that require authentication sequences, because an intruder could replay legitimate authentication sequence messages to gain access to a system. Packet replay is frequently undetectable, but can be prevented by using packet time stamping and packet sequence counting.

Eavesdropping: This allows a cracker (hacker) to make a complete copy of network activity. As a result, a cracker can obtain sensitive information such as passwords, data, and procedures for performing functions. It is possible for a cracker to eavesdrop by wiretapping, using radio, or using auxiliary ports on terminals.

Intrusion attacks: In these attacks, a hacker uses various hacking tools to gain access to systems. These can range from password-cracking tools to protocol hacking and manipulation tools.

Intrusion detection tools often can help to detect changes and variants that take place within systems and networks.

Network spoofing: In network spoofing, a system presents itself to the network as though it were a different system (computer A impersonates computer B by sending B's address instead of its own). The reason for doing this is that systems tend to operate within a group of other trusted systems.

2.3.6 Ways of dealing with the security of electronic information

According to Obaidat (2009), data to be accessed via communication networks or transmitted over public networks must be protected against unauthorized access, misuse, and modification. He further states that security protection requires three mechanisms: enablement, access control, and trust management. Enablement implies that a cohesive security policy has been implemented and that an infrastructure to support the verification of conformance with the policy is deployed. Perimeter control determines the points of control, the objects of control and the nature of control to provide access control and perform verification and authorization. Trust management allows the specification of security policies relevant to trust and credentials. It ascertains whether a given set of credentials conforms to the relevant policy, delegates trust to third parties under relevant conditions, and manages dynamically, if needed, the level of trust assigned to individuals and resources in order to provide authorization.

He further states that, public key infrastructures (PKIs) represent an important tool to be used in enablement, while biometric-based infrastructures are gaining an important role in providing robust access control. Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic. Biometric-based solutions are able to provide for confidential financial transactions and personal data privacy. The need for biometrics can be found in electronic governments, in the military, and in commercial applications. In addition, trust management systems start to be used in a large set of environments such as electronic payment and healthcare management, where transactions and accesses are highly sensitive.

Data that can be accessed on a network or that are transmitted on the network, from one edge node to another, must be protected from fraudulent modification and misdirection, typically information security systems require three main mechanisms to provide adequate levels of electronic mitigation (Obaidat, 2009).

2.4 Human resource in the context of information security

According to Kaufman (2008), Human resources are the people who make up the workforce of an organization, business sector, or economy. Human resources is used to describe both the people who work for a company or organization and the department responsible for managing resources related to employees.

According to Scott (2018), the human resources department is a department that handles a range of different functions within an organization, the department is responsible for hiring and firing employees, training workers, maintaining interoffice relationships and interpreting employment laws and also works diligently behind the scenes to ensure an organization runs efficiently.

According to code of practice, human resource management can be evaluated based on two general ideas which are legal agreement and security training or awareness program for the staff, the purpose of this is to minimize the risks of human error, theft, fraud or misuse of facilities and also to ensure that users are aware of any security threats and concerns, in that they are fully prepared to support the corporate security policy in their routines activities (Rahman, 2013).

Human errors, carelessness and greediness are responsible for most thefts, frauds or misuse of facilities, various proactive measures that should be taken are, to make personnel screening policies, confidentiality agreements, terms and conditions of employment, and information security education and training (Rahman, 2013).

The Human Resource department's responsibility is critical in cyber security. The IT department must work closely with your HR department to safeguard all employee files; ideally, they should be encrypted and secured and, if there are employees who work remotely from home or in other offices, HR needs to be able to establish policies that cover how they can access the organization's computers, data, files, and many others (Dimoff, 2018).

2.5 Information security objectives

This section analyses information security objectives as understood by different authors, experts. The information security objectives include; Confidentiality, Integrity, Availability, Non-repudiation, Authorization, Authentication, and Accountability.

2.5.1 Confidentiality

According to Laudon (2008), confidentiality is the ability to ensure that messages and data are available only to those who are authorized to view them, on the other hand, Gibson (2012), states that confidentiality is a mechanism for managing feelings of incompetence and the concomitant

risk of embarrassment that can arise in everyday social situations, for example, in the encounter between health care professional and client. He further states that confidentiality protects the dignity and rights of the participant and minimize the risk of harm. However the International Organization for Standardization/ international standard organization (ISO) in ISO-17799 asserts that confidentiality is ensuring that information is accessible only to those authorized to have access to it. It is one of the cornerstones of information security. Confidentiality is one of the design goals for many cryptosystems, made possible in practice by the techniques of modern cryptography.

According to Kabay (2004), confidentiality pertains to the treatment of information that an individual has disclosed in a relationship of trust and with the expectation that it will not be divulged to others without permission in ways that are inconsistent with the understanding of the original disclosure. Kabay (2004) further noted that confidentiality is about identifiable data, an extension of privacy, an agreement about maintenance and who has access to identifiable data If applicable, subjects are be informed of the precautions that will be taken to protect the confidentiality of the data and which parties will or may have access (for instance, research team), this will allow subjects to decide about the adequacy of the protections and the acceptability of the possible release of private information to the interested parties. In doing so, confidentiality is ensured while Schou (2007), states that confidentiality ensures that information is not disclosed to unauthorized persons, processes, or devices. This factor requires discrete functions such as information labeling and the establishment of need-to-know rules. Confidentiality is related to privacy. Privacy is usually considered to be associated with protection of personal information and according to Clark (2006), confidentiality is understood to mean that the personal information that the worker gathers about the client will not be communicated to other persons or organizations except with the client's consent and only insofar as strictly necessary for the agreed purposes of the work in hand.

On the other hand according to Shardlow (1995: 66-7), confidentiality may be taken as an exhortation to keep secret both written and verbal communication from clients, it is expected that social workers will not divulge information to others except in certain specified circumstances. Confidentiality ensures that information is accessible only to those authorized to have access to it, in information security, confidentiality "is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes (Shardlow, 1995: 66-7). However Taherdoost (2013) states that confidentiality is the protection of information from unauthorized access. This goal of the CIA triad emphasizes the need for information protection. Confidentiality requires measures to ensure that only authorized people are allowed to access the

information. For example, confidentiality is maintained for a computer file if authorized users are able to access it, while unauthorized persons are blocked from accessing it Confidentiality in the CIA triad relates to information security because information security requires control on access to the protected information. Confidentiality is more important than the other goals when the value of the information depends on limiting access to it. For example, information confidentiality is more important than integrity or availability in the case of proprietary information of a company. Also, confidentiality is the most important when the information is a record of people's personal activities. To guarantee confidentiality under the CIA triad, communications channels must be properly monitored and controlled to prevent unauthorized access (Andress, 2014).

2.5.2 Integrity

According to Laudon (2008), in information security, data integrity means maintaining and assuring the accuracy and completeness of data over its entire life-cycle. This means that data cannot be modified in an unauthorized or undetected manner. Integrity refers to the ability to ensure that information being displayed on a website, or transmitted or received over the internet, has not been altered in any way by unauthorized party. For example, if unauthorized person intercepts and changes the content of an online communication such as by redirecting a bank wire transfer into a different account, the integrity of the message has been compromised because the communication no longer represents what the original sender intended however, Boritz (2011), states that in an age where information is widely available, and that it is difficult to determine whether information is valid or correct, and that any internet search can turn up dozens of differing opinions, studies and documents about a topic that all claim to be accurate. A document has integrity when nothing has been altered, added or deleted; it represents exactly what was created by its author. Organizations can only control information they create and manage; thus, they have the opportunity and responsibility to protect the integrity of that information.

Boritz (2011), further states that integrity policies should prevent accidental or malicious changes or the destruction of information, a concept that has long been recognized as important in the IT industry. However, the concept of integrity is somewhat difficult to understand. To ensure integrity, organizations should make sure their documents, information or data are: accurate and free from error or defect, consistent with a standard rule or policy, unmodified and never changed in any form, meaning or character, consistent and uniform over its life cycle, used only by authorized people using authorized processes, include an audit trail that tracks its life cycle.

Integrity of information refers to protecting information from being modified by unauthorized parties. Information only has value if it is correct. Information that has been tampered with could prove costly. For example, if you were sending an online money transfer for $100, but the information was tampered in such a way that you actually sent $10,000, it could prove to be very costly for you. As with data confidentiality, cryptography plays a very major role in ensuring data integrity. Commonly used methods to protect data integrity include hashing the data you receive and comparing it with the hash of the original message. However, this means that the hash of the original data must be provided to you in a secure fashion. More convenient methods would be to use existing schemes such as Gnu Privacy Guard (GPG) to digitally sign the data (Peltier, 2002).

2.5.3 Availability

According to Boritz (2011), for any information system to serve its purpose, the information must be available when it is needed, this means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Availability is the situation where information is available when and where it is rightly needed. The main concern in the CIA triad is that the information should be available when authorized users need to access it. Availability is maintained when all components of the information system are working properly. Problems in the information system could make it impossible to access information, thereby making the information unavailable. In the CIA triad, availability is linked to information security because effective security measures protect system components and ensuring that information is available (Shabtai, 2012).

Availability of information refers to ensuring that authorized parties are able to access the information when needed. Information only has value if the right people can access it at the right times. Denying access to information has become a very common attack nowadays. Almost every week you can find news about high profile websites being taken down by Distributed Denial-of-Service (DDoS) attacks. The primary aim of Distributed Denial-of-Service (DDoS) attacks is to deny users of the website access to the resources of the website. Such downtime can be very costly. Other factors that could lead to lack of availability to important information may include accidents such as power outages or natural disasters such as floods. How does one ensure data availability? Backup is key. Regularly doing off-site backups could limit the damage caused by damage to hard drives or natural disasters. For information services that is highly critical, redundancy might be appropriate. Having an off-site location ready to restore services in

case anything happens to your primary data centers will heavily reduce the downtime in case of anything happens (Layton, 2007). Availability is ensuring timely and reliable access to and use of information. It is also the property of being accessible and useable upon demand by an authorized entity (Layton, 2007).

2.5.4 Non-repudiation

Non-repudiation in the information security context refers to one of the properties of cryptographic digital signatures that offer the possibility of proving whether a particular message has been digitally signed by the holder of a particular digital signature's private key. Non-repudiation is a somewhat controversial subject, partly because it is an important one in this day and age of electronic commerce, and because it does not provide an absolute guarantee: a digital signature owner, who may like to repudiate a transaction maliciously, may always claim that his or her digital signature key was stolen by someone and that someone actually signed the digital transaction in question, thus repudiating the transaction. It is a way of guaranteeing that people cannot deny that an event happened or an action was carried out by an entity (International Standard Organization (ISO) 14516: 2002).

Non-repudiation is the assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information CNSSI-4009; SP 800-60). It is protection against an individual falsely denying having performed a particular action. Non-repudiation provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message (SP 800-53; SP 800-18). Non-repudiation is the security service by which the entities involved in a communication cannot deny having participated. Specifically, the sending entity cannot deny having sent a message (non-repudiation with proof of origin), and the receiving entity cannot deny having received a message (non-repudiation with proof of deliver (FIPS 191). A service that is used to provide assurance of the integrity and origin of data in such a way that the integrity and origin can be verified and validated by a third party as having originated from a specified entity in possession of the private key (i.e., the signatory) (FIPS 186).

2.5.5 Authorization

Authorization is the process of ensuring that a user has sufficient rights to perform the requested operation and preventing those that are without sufficient rights from doing the same. (International Standard Organization ISO 14516: 2002). Authorization implies access privileges that are granted to; a user, program, or process or the act of granting those privileges after

logging into a system, the user may try to issue commands. The authorization process determines whether the user has the ultimate authority to issue such commands. In simple terms, authorization is the process of enforcing policies: determining what types or qualities of activities, resources, or services a user is permitted. Authorization usually occurs within the context of authentication. Once you have authenticated a user, he or she may be authorized for different types of access or activity (Rouse, 2010).

2.5.6 Authentication

Authentication is a method that is used for proving that you are who you say you are. Strong authentication is the use of two or more different authentication methods, such as a smart card and a Personal Identification Number (PIN), or a password and a form of biometrics, such as a fingerprint or retina scan. Authentication is a process that is used to confirm that a claimed characteristic of an entity is indeed correct. To authenticate is to verify that a characteristic of attribute that appears to be true is in fact true (International Standard Organization (ISO) 14516: 2002). Authentication involves Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. Authentication is the process of establishing confidence of authenticity Authentication encompasses identity verification, message origin authentication, and message content authentication.

2.5.7 Accountability

Accountability is the process of measuring the resources a user consumes during accessibility. This may include the amount of system time or the amount of data a user has sent and/or received during a session. Accountability can be carried out by logging of session statistics and information usage and is used for the purpose of authorization control, billing, trend analysis, resource utilization, and capacity planning activities (Rouse, 2010). It also implies that information usage should be transparent so that it is possible to determine whether a particular use is appropriate under a given set of rules and that the system enables individuals and institutions to be held accountable in case of any misuse (Kagal, 2008).

Accountability is the state of being answerable for the actions and decisions that have been assigned to an entity. If a user of data makes a decision adverse to the consumer (such as denial of a loan or rejection of an employment application) the decision must be justified with reference to the specific data in the credit report on which the decision was based (accountability) (Solove, 2004). Accountability appliances can serve as proxies to data sources, mediating access to the data, and maintain provenance information and logs of data transfers (Szomszor, 2003).

Accountability is the security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action (International Standard Organization ISO 14516: 2002). Accountability is a principle that an individual is entrusted, to safeguard and control, keying material, and information and is answerable to authority for the loss or misuse of that equipment or information.

2.6 Information security controls

This section points out information security controls as understood and discussed by different authors/experts.

2.6.1 Ongoing knowledge of attack sources, scenarios, and techniques:

According to Clark (2016), all defensive measures are based on knowledge of the attacker's capabilities and goals, maintenances of an ongoing awareness of attack threats through security information sources, as well as the probability of attack.

2.6.2 Up-to-date equipment inventories and network maps:

According to Kurtz (2016), inventories of hardware and the software on each system can accelerate the institution's response to newly discovered vulnerabilities and support the proactive identification of unauthorized devices or software.

2.6.3 Rapid response capability to react to newly discovered vulnerabilities:

According to Durbin (2016), institutions need to have a reliable process so as to become aware of new vulnerabilities and to react as necessary to mitigate the risks posed by newly discovered vulnerabilities. Durbin further states that software is seldom flawless and that some of the flaws may represent security vulnerabilities and in some cases, management may mitigate the risk by reconfiguring other computing devices, there is need for rapid response because a widely known vulnerability is subject to an increasing number of attacks.

2.6.4 Network access controls over external connections:

Typically, firewalls are used to enforce an institution's policy over traffic entering the institution's network, firewalls are also used to create a logical buffer, called a Demilitarized Zone (DMZ), where servers are placed that receive external traffic, the DMZ is situated between the outside and the internal network and prevents direct access between the two (Fratto, 2007).

2.6.5 System hardening:

Computer equipment and software are frequently shipped from the manufacturer with default configurations and passwords that are not sufficiently secure with in an institutional environment, this therefore requires hardening the systems prior to placing them in a production environment. System "hardening" is the process of removing or disabling unnecessary or insecure services and files, a number of organizations have current efforts under way to develop security benchmarks for various vendor systems (Fratto, 2007).

2.6.6 Controls to prevent malicious code:

Educating employees in safe computing practices, installing anti-virus software on servers and desktops, maintaining up-to-date virus definition files, and configuring systems protects against the automatic execution of malicious code, malicious code can deny or degrade the availability of computing services; steal, alter, or insert information; and destroy any potential evidence for criminal prosecution, types of malicious code include viruses, worms, and Trojan Horses (Ballou, 2003).

2.6.7 Rapid intrusion detection and response procedures:

When a security failure occurs and an attacker is "in" the institution's system, only rapid detection and reaction can minimize any damage that might occur, techniques used to identify intrusions include; Intrusion Detection Systems (IDS) for the network and individual servers (i.e., host computer), automated log correlation and analysis, and the identification and analysis of operational anomalies (Scarfone, 2007).

2.6.8 Physical security of computing device:

Bhaskar (2008), states that those security elements necessary to ensure that unauthorized persons are excluded from physical spaces and assets where their presence represents a potential threat. All types of computers, computing devices and associated communications facilities must be considered as sensitive assets and spaces and be protected accordingly. Examples of physical security controls are physical access systems including guards and receptionists, door access controls, restricted areas, closed-circuit television (CCTV), automatic door controls and human traps, physical intrusion detection systems, and physical protection systems. Administrative and technical controls depend on proper physical security controls being in place.

2.6.9 Authorized use policy:

According to Jøsang (2017), a policy addresses the systems which various users can access, the activities they are authorized to perform, prohibitions against malicious activities and unsafe computing practices, and consequences for noncompliance.

2.5.10 Training:

According to Banzhaf (1998), institutions need to come up with processes to identify, monitor, and address training needs training personnel in the technologies they use and the institution's rules governing the use of those technologies. Technical training is particularly important for those who oversee the key technology controls such as firewalls, intrusion detection, and device configuration. Security awareness training is important for all users.

2.6.11 Independent testing:

According to Kurtz (2016), having a testing plan that identifies control objectives; schedules tests of the controls used to meet those objectives; ensures prompt corrective action where deficiencies are identified; and provides independent assurance for compliance with security policies security tests are necessary to identify control deficiencies, an effective testing plan identifies the key controls, then tests those controls at a frequency based on the risk that the control is not functioning. Security testing should include independent tests conducted by personnel without direct responsibility for security administration, adverse test results indicate that a control is not functioning and cannot be relied upon, follow-up can include correction of the specific control, as well as a search for, and correction of, a root cause. Types of tests include audits, security assessments, vulnerability scans, and penetration tests (Kurtz, 2016).

2.7 Information security challenges

This section brings out information security challenges as analyzed by different authors/experts.

2.7.1 Compromised credentials and device:

While malware has certainly evolved to become more sophisticated and dangerous than ever, business leaders must "look beyond" it if they hope to improve their information security standards (Kurtz, 2016).

"If you look for malware you won't see breaches using legitimate credentials," simply hackers steal login information and use the credentials to access applications and sensitive data and as a

result, it's hard to identify when organizations are breached, many have lost data, only to discover those intrusions months and years later (Kurtz, 2016).

2.7.2 Lateral hacker movement/breach containment:

Once cybercriminals find their way inside corporate networks, they're moving laterally between applications until they find the most sensitive and valuable data, cryptographic isolation and end-to-end encryption prevents lateral movement (Gartner, 2016).

2.7.3 Stitched-together security:

According to Clark (2016), security Frankenstein is a major information security concern, in other words, by using mismatched, cobbled-together security solutions instead of one holistic product, organizations are putting data at risk. Businesses and associations should try to find a single cyber security solution that effectively meets all needs, such as one that combines cryptographic segmentation and role-based access control in a package that meets all information security needs.

2.7.4 Vulnerabilities can turn into intrusion points:

Heart bleed, poodle, Sandworm and Shellshock are not Hollywood blockbusters. They are systemic vulnerabilities that cyber criminals take advantage of. Steve Durbin, managing director of the Information Security Forum, a nonprofit that analyzes cyber threats, told Chief information officer (CIO) that a "pervasive technology monoculture" is to blame for many attacks. Because some IT solutions are so popular, once vulnerability is discovered, cyber criminals can launch attacks on multiple organizations without changing their strategies (Durbin, 2016).

2.7.5 The age of cybercrime syndicates:

Durbin (2016), states that ever since the birth of the Internet, crime syndicates saw value in exploiting worldwide connectivity. Now, Durbin explained that they have big budgets, deep skill sets and sophisticated tools to circumvent many of the best cyber security solutions. Keeping an eye on these syndicates will be a key to information security success.

2.7.6 Threats on the home front:

The biggest threat to corporate and private data has nothing to do with technology; in fact, the source noted that 25 percent of cyber incidents reported are labeled "non-cyber," topping the list

of data breach causes which means implementing internal network security solutions such as encryption might be the best defense in regard to information security (Nevias, 2016).

2.7.7 Other challenges in Information Security are people and access control:

One of the primary causes of most data breaches and security incidents are people unintentionally doing something they should not or not having the proper access controls on a system or the associated data. These challenges can be addressed by properly classifying and encrypting data, having a security awareness training program and limiting access to systems and data as much as possible (Nevias, 2016).

2.8 Related studies

Information security is concerned with protecting the confidentiality, integrity and accessibility of information (National Institute of Technical Standards, 1995). The 2002 Computer Crime and Security Survey, conducted by the Computer Security Institute (CSI) and Federal Bureau of Investigation (FBI) in Wall Street, reported that 90% of respondents detected computer security breaches within the past year (Power, 2002), Discussions concerning corporate information security breaches, however, provide conflicting views about the economic impact of such breaches. Some press reports and survey results suggest that firms experience significant financial losses as a result of information security breaches (Kedrosky, 2000). Others, however, suggest that security systems effectively prevent breaches with severe economic consequences, and the breaches that do occur are nuisances with inconsequential economic effects on firms (Smith, 2000).

An alternative argument, however, suggests that the economic consequences of information security breaches are trivial over the long run. The intuition underlying this argument is that firms protect their most valuable information assets at a higher level than their less valuable information. That is, since all information cannot be protected to the point where there is zero probability of a security breach, firms may allocate their security expenditures in a manner that minimizes the economic impact of security breaches (Gordon & Loeb, 2001).

The risk management perspective: information security measures reduce the risk of unwanted incidents. Failures of information security are clearly adverse events which cause losses to businesses; information security is thus a risk management discipline that manages the cost of information risk to the business (Blakely et al., 2001). In this perspective, effectiveness is understood as the ability of a measure to reduce risk to an acceptable level.

The economic perspective: information security measures give positive return of investment; an economic approach to information security was suggested by Gordon & Loeb (2001), who have developed an economic model for information security. Gordon & Loeb (2001), argue that a company should maximize the expected benefits from investment to protect their information. In this perspective, effectiveness of information security measures is understood as the ability of a measure to give a positive return of investment, i.e. the ratio of money gained relative to the amount of money invested.

The legal perspective: information security measures avoid violations of legal requirements. Efforts must be made to meet legal requirements, which in turn should prevent possible security breaches (Lobree, 2002). In this perspective effectiveness is understood as the ability of a measure to assist the organization to meet legal requirements. The cultural perspective: information security measures create a good security culture. In this perspective, effectiveness is understood as the influence of a measure on individual and organizational awareness and behaviour in a positive direction.

The four perspectives are clearly interrelated, although they describe different expectations of the performance of the information security measures. How legal and regulatory requirements are met will for instance depend more on people and procedures than on technical security measures. What is needed is the right combination of measures that reduce the business risks to an acceptable level and at the same time ensure compliance to the law (Sundt, 2006; Berghel, 2005).

Several authors have studied the effectiveness of the information security policy. The effectiveness of the policy is dependent on the way the security contents are addressed in the policy document and how the content is communicated to users (Ho¨ne & Eloff, 2002). Kemp (2005) argues that a security policy is not effective unless it is supported by the management, Thomas & Solms (2006**)** also add that effectiveness is created when the policy is adopted by employees in practical actions**,** Doherty & Fulford (2006) argue that the specific alignment of the information security policy with the strategic information system plan might be one constructive way of making the policy more relevant for managers.

According to Karyda (2005), the organizational characteristics play an important role for the successful implementation and adoption of the security policy. The success criteria are to have a coherent organization where employees follow a code of best practice or a culture where employees participate in the security work. Wiant (2005) views the security policy as a deterrent measure, and argues that the information security policy is effective when computer abuse incidents and the seriousness of those incidents are reported.

Siponen (2000) & Albrechtsen (2007) show that although information security guidelines are of a prescriptive nature and imperative to the users, users often fail to apply them as intended. As a result, the guidelines are often not effective for the purpose of influencing human behaviour and attitudes. People are an important resource in coping with information security, as the success of an information security programme depends on the commitment from all users. If this commitment is not in place, the security mechanisms could be bypassed or diminished by employees (Ward & Smith, 2002; Schneier, 2000).

Thomson & Solms (2006), claim in an ambitious manner that to achieve effectiveness, information security should be transferred into tacit knowledge and unconscious consciousness. Security awareness programmes are one method to raise users' knowledge and commitment. Johnson (2006) argues that there are several beneficial effects of a security awareness programme: increased confidence, better protection, correctness and reliability of information, fewer internal undesired incidents, improved moral and detection capability and improved compliance with laws and regulations. Information security includes organizational aspects, legal aspects, institutionalization and applications of best practices in addition to security technologies (Solms, 2006; Siponen & Oinas-Kukkonen, 2007). A study by Siponen & Oinas-Kukkonen (2007) reveals that research on information security traditionally has been dedicated to technological aspects, and that more research on the non-technical aspects is needed.

2.9 Research gap

Firms protect their most valuable information assets at a higher level than their less valuable information. That is, since all information cannot be protected to the point where there is zero probability of a security breach, firms may allocate their security expenditures in a manner that minimizes the economic impact of security breaches (Gordon & Loeb, 2000).

CHAPTER THREE

METHODOLOGY

3.0 Introduction

In this chapter, the researcher explains the methods and techniques which were used while gathering, analyzing, interpreting and presenting data. It contains the research design, the research population, the sample size and sampling procedures, research instruments for data collection, Validity, Reliability and the procedures for data gathering and analysis, ethical considerations, and limitations of the study.

3.1 Research design

According to Ahuja (2001), a research design is a detailed plan of how the goals of research will be achieved. According to Creswell (2009), research designs are plans and the procedures for research that span the decisions from broad assumptions to detailed methods of data collection and analysis. The research was based on correlation design (according to Amin (2005), a correlation study describes in quantitative terms the degree to which variables are related). Simple correlation study was used to establish if there was a relationship between security objectives and challenges to information security at KIU. This was because the study focused on ascertaining if there was a significant relationship between security objectives and challenges to information security of records at KIU. In this research quantitative approach to research was used. Quantitative research refers to the type of research which involves the collection of numerical data in order to explain, predict and control phenomena of interest, data analysis being mainly statistical (Amin, 2005).

3.2 Research population

According to Amin (2005), population is the aggregation of items or objects from which samples are drawn, constituting the entire collection of observations to which study results generalize. According to Oso (2009), target population refers to the total number of subjects, or the total environment of interest to the researcher. In this study, the target population was seventy eight (78) respondents and these included KIU administrators specifically, Directors, Deputy Directors, Administrators, Teaching and Learning coordinators (TLCs), Department Examination coordinators (DECs), Heads of departments, staff within the records, Library, and Information and Communication Technology (ICT) department, at Kampala International University, main campus, Kampala - Uganda. The departments that participated in the research included admissions, records, library, marketing, Information and Communication Technology

(ICT), Quality assurance (QA), school of engineering and applied science (SEAS), school of Computing and Information Technology (SCIT), School of Law, and College of humanities and social sciences. The above were chosen because the research was so specific.

Table 3.2.1: Target population distribution per each department

No.	Departments	Target Population
1.	Marketing	3
2.	Library	4
3.	ICT	8
4.	SCIT	8
5.	SEAS	14
6.	Law	17
7.	QA	3
8.	Admissions	2
9.	Records	5
10.	Humanities	14
	Total	**78**

Source: primary data, 2017

The above table 3.2.1 shows the target population of seventy eight (78) administrative staff and they included Directors, Deputy Directors, Administrators, Teaching and Learning coordinators (TLCs), Department Examination coordinators (DECs), Heads of departments, staff within the records, Library, and Information and Communication Technology (ICT) department, at Kampala International University, main campus, Kampala - Uganda. Departments that participated in the research included admissions, records, library, marketing, Information and Communication Technology (ICT), Quality assurance (QA), school of engineering and applied science (SEAS), School of Computing and Information Technology (SCIT), School of Law, and College of humanities and social sciences.

3.3 Sample size

The sample size is the number of entities (subjects, etc.) in a subset of a population selected for analysis. The Sloven's formula was used to determine the minimum sample size.

The formula is $n = N/1+N\,(e)^2$

Where 'n' was the sample size, 'N' was the population size and 'e' was the level of significance which was equivalent to 0.05.

n = 78 /1+78(0.05)2

n=78/1+78(0.0025)

n=78/1+0.195

n=78/1.195

n= 65

3.4 Sampling procedure

A sample of respondents was selected through purposive sampling and random sampling. The researcher gathered data from respondents thought to be having more knowledge about information security issues at KIU, main campus. According to Amin (2005), simple random sampling is a sampling technique where by samples of the same size have an equal chance of being selected. According to Mugenda and Mugenda (1999), purposive sampling is a sampling technique that allows the researcher to use cases that have the required information with respect to the objectives of his or her study. Simple random sampling and purposive sampling techniques were used, because there was need to gather data from specific respondents who really understand information security of records. In this study Directors, Deputy Directors, Administrators, Teaching and Learning coordinators (TLCs), Department Examination coordinators (DECs), Heads of departments, staff within the records, Library, and Information and Communication Technology (ICT) department, were the targeted respondents.

3.5 Research instrument

Questionnaires were used to gather data from the different respondents. A Questionnaire is a set of related questions meant to engage a respondent or respondents with a view of getting information or a research tool or technique for primary data collection containing questions that is according to Mubazi (2009/10). Questionnaires were used because of the advantages they have which include the following below.

Large amounts of information can be collected from a large number of people in a short period of time and in a relatively cost effective way, the results of the questionnaires can usually be quickly and easily quantified by either a researcher or through the use of a software package, the questionnaires can be analyzed more scientifically and objectively than other forms of research, when data has been quantified, it can be used to compare and contrast other research and may be used to measure change and lastly, quantitative data can be used to create new theories and / or test existing hypotheses.

The questionnaire comprised of two sections, the first section consisted of the introduction and the personal profile of respondents and the second section comprised of information security objectives, controls, and challenges in Kampala International University.

There were also informal interactions with the respondents. This enabled the researcher to gather direct response from the respondents.

3.6 Validity

Validity is the ability to produce findings that are in agreement with theoretical or conceptual values; in other words, to produce accurate results and to measure what is supposed to be measured (Amin, 2005). The researcher worked hand in hand with the supervisor and another subject expert to adjust the research instrument. The researcher tested the validity of the instrument. The items were rated as follows; 4 – very relevant, 3 – quite relevant, 2 – somewhat relevant and 1 – not relevant.

The researcher then put the items into two groups with 1&2 in one group and 3&4 in the same group, and then calculated the content validity index using the formula below.

$$CVI = \frac{\text{items rated as very relevant and quite relevant (3\&4)}}{\text{Total number of items}}$$

For the instrument to be valid the average index should be 0.7 or above.

For information security controls the content validity index (CVI) was as follows.

There were 32 questions in the questionnaire, 28 were very relevant, and 2 were quite relevant whereas 2 questions was somewhat relevant

The CVI for information security objectives was, (28+2)/32

CVI=30/32

CVI=0.9375

For information security objectives the content validity index (CVI) was as follows.

There were 35 questions in the questionnaire, 30 were very relevant, and 4 were quite relevant whereas 1 question was somewhat relevant

The CVI for information security objectives was, (30+4)/35

CVI=34/35

CVI=0.971

For information security challenges the content validity index (CVI) was as follows.

There were 8 questions in the questionnaire, 6 were very relevant, and 1 was quite relevant whereas 1 questions was somewhat relevant

The CVI for information security challenges was, (6+1)/8

CVI=7/8

CVI=0.875

The questionnaire was valid because all the content validity index above were above 0.7

3.7 Reliability

According to Brown (2007), item analysis employing the cronbach coefficient alpha permits the researcher to test reliability of sets of items in order to examine the effects of dropping or adding individual items to a test. Ideally, a test used to assess treatment outcomes should have a reliability of 0.9 or higher Brown (2007).

The reliability of the instruments was tested and the Cronbach's alpha was 0.944 which showed that the questionnaire was reliable.

Table 3.7.1: Case processing summary

Case processing summary

		N	%
Cases	Valid	52	100.0
	Excluded[a]	0	0.0
	Total	52	100.0

Source: primary data, 2017

a. Listwise deletion based on all variables in the procedure.

Table 3.7.2: Reliability statistics

Reliability statistics

Cronbach's Alpha	N of Items
0.944	79

Source: primary data, 2017

This table gives the Cronbach's alpha. In this case, $\alpha = 0.944$, which show that the Questionnaire was reliable

3.8 Data gathering procedures

Data collection was done after a sequence of the following steps:

1. An introductory letter was obtained from College of Higher Degrees and Research, Kampala International University which the researcher used to solicit approval to conduct research from the institution.
2. The respondents were given explanation about the purpose of the study and were requested to sign the Informed Consent Form.
3. More than enough questionnaires were reproduced for distribution.

During the administration of the questionnaires

The respondents were requested to answer all the questions in the questionnaires and not to leave any part of the questionnaires unanswered.

After the administration of the questionnaires

The data gathered was collated, encoded into the computer and statistically treated using the Statistical Package for Social Scientists (SPSS) version.

3.9 Data analysis

Analysis of data was made with the use of Statistical Package for Social Scientists (SPSS) version 16.0 as a tool for analyzing the data. The study used frequencies and percentages to analyze the profile of respondents and descriptive statistics to analyze the extent of compliance to information security objectives, information security controls, and challenges of information security of records at Kampala International University. Pearson Linear Correlation Co-efficiency (PLCC) was used to establish if there was a significant relationship between security objectives and challenges of information security of records in KIU.

3.10 Ethical considerations

Bearing in mind the ethical issues, the researcher provided the respondents with the necessary information as regards to the main purpose of the research, expected duration and how they were to fill the questionnaires and were also informed that confidentiality of their responses was to be ensured.

3.11 Limitations

As far as the limitations are concerned, it was not easy to collect data from some respondents that is, they were not co-operative fearing that their responses would be exposed. There was poor response ratio. Some respondents took a long time to respond to the questionnaires.

3.12 Delimitations

Respondents were assured of confidentiality by the researcher in as far as their responses were concerned. The researcher kept on going to the respondents' offices until when they filled the questionnaires and returned them to the researcher.

CHAPTER FOUR

DATA PRESENTATION AND ANALYSIS

4.0 Introduction

The results in this section were presented so as to explore the data with respect to the research study objectives. The data was captured, entered, coded and analyzed using the Statistical Package for Social Scientist (SPSS) software.

The analysis was done using frequencies and percentages, descriptive statistics that is means and standard deviation and also Pearson Linear Correlation Co- efficiency (PLCC) was used to establish if there is a significant relationship between information security objectives and challenges to information security at KIU. The researcher chose those measures because they were the ones suitable for the study. Sixty five questionnaires were distributed but only fifty two of them were returned. The researcher looked at; Profile of the respondents, Descriptive statistics for determining the extent of compliance to information security objectives at KIU, Descriptive statistics to establish information security controls at KIU, Descriptive statistics to investigate challenges of information security of records in KIU, Pearson Linear Correlation Co- efficiency (PLCC) was used to ascertain if there was a significant relationship between challenges to information security and security objectives at KIU.

4.1 Profile of the respondents

This was characterized by Gender, Age, Education and Working duration. The researcher made a walk through all the information obtained and summarized it so as to get conclusive results as seen in the table below.

Table 4.1.1: Profile of the respondents per each department that responded to the questionnaires

No.	Departments	Respondents
1.	Marketing	1
2.	Library	3
3.	ICT	7
4.	SCIT	2
5.	SEAS	6
6.	Law	12
7.	QA	2
8.	Admissions	1
9.	Records	5
10	Humanities	13
	Total	**52**

Source: primary data, 2017

There was poor response ratio, the researcher expected 100% response but only received 80% which meant that some respondents were either too busy or were not aware of what was being asked within the questionnaire.

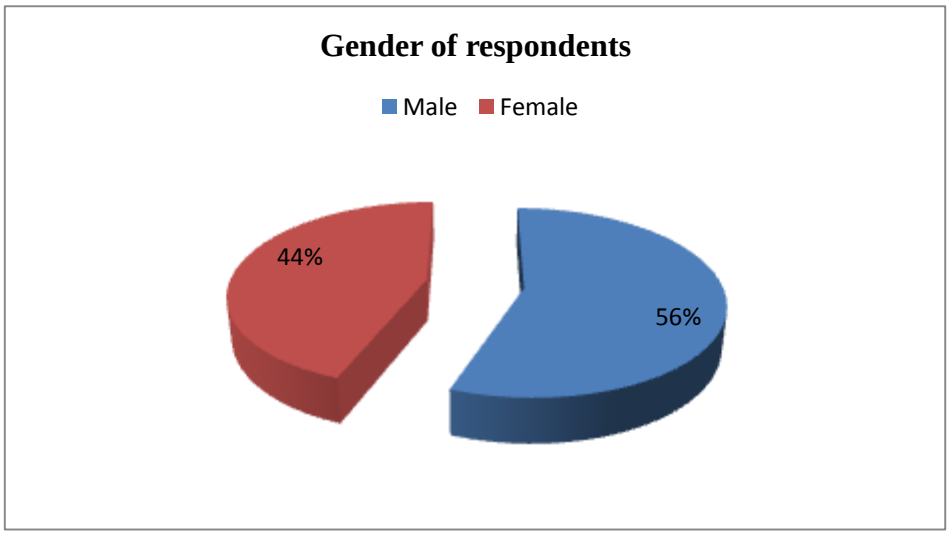
Table 4.1.2: Profile, frequency and percentage of the respondents

No.	**Categories**	**Frequency**	**Percentage (%)**
1.	**Gender** Male	29	55.8
2.	Female	23	44.2
	Total	52	**100.0**
1.	**Age** 20-29	25	48.1
2.	30-49	20	38.5
3.	50 and above	7	13.5
	Total	**52**	**100.0**
1.	**Education qualifications** Certificate	2	3.8
2.	Diploma	8	15.4
3.	Undergraduate degree	18	34.6
4.	Postgraduate degree	24	46.2
	Total	**52**	**100.0**
1.	**Work experience** 0-5 Years	8	15.4
2.	5-10years	34	65.4
3.	10years +	10	19.2
	Total	**52**	**100.0**

Source: primary data, 2017

Table 4.1.2 shows the profile of the respondents characterized by Gender, Age, Education and Working duration. The researcher made a walk through all the information obtained and summarized it so as seen above.

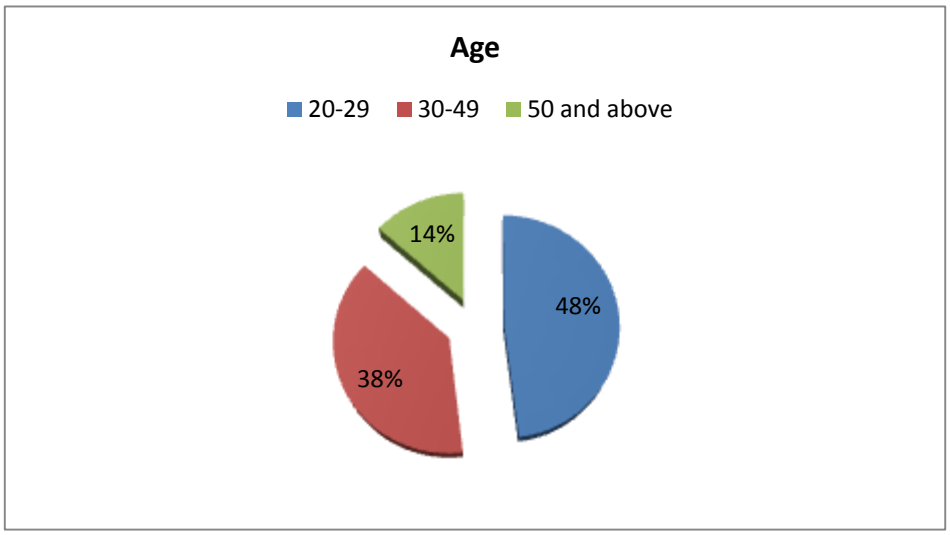
Figure 4.1.1: Percentage distribution of gender of the respondents



Source: primary data, 2017

Figure 4.1.1 indicates that majority of the respondents were male 29 (56%) while the female were 23 (44%). The findings indicate that Kampala International University employs more male than female. From the informal interactions with the respondents they mentioned that they prefer working with male to female because they perceive that male employees are more committed and can easily deal with Information security related issues than female.

Figure 4.1.2: showing age distribution of the respondents

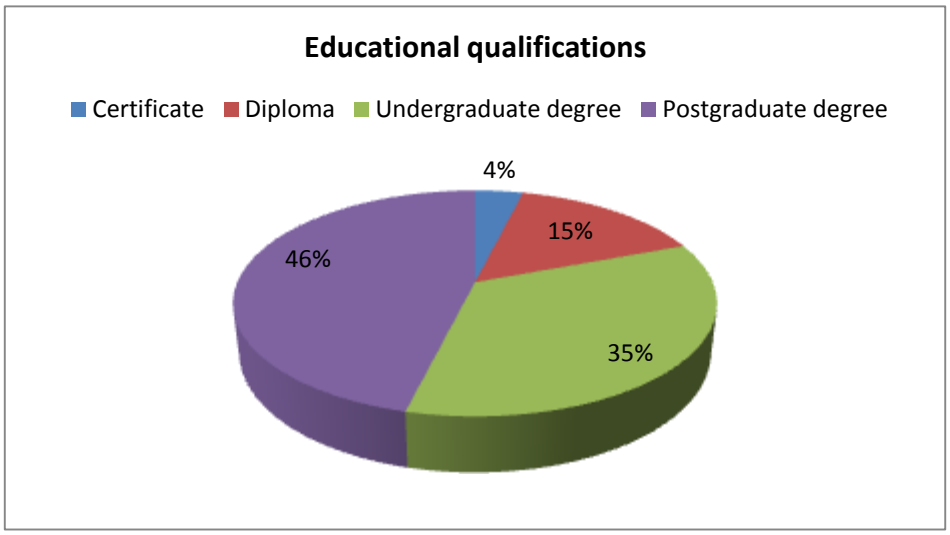


Source: primary data, 2017

The findings indicated that, majority of the respondents were between the age of 20-29, and they were 25(48%) while the least were between the ages of 50 and above, these were 7(14%). Those

between 30-49 years were 20 (39%). This implied that the respondents between the ages of 20-29 knew a lot about information security more than respondents within the other age brackets.

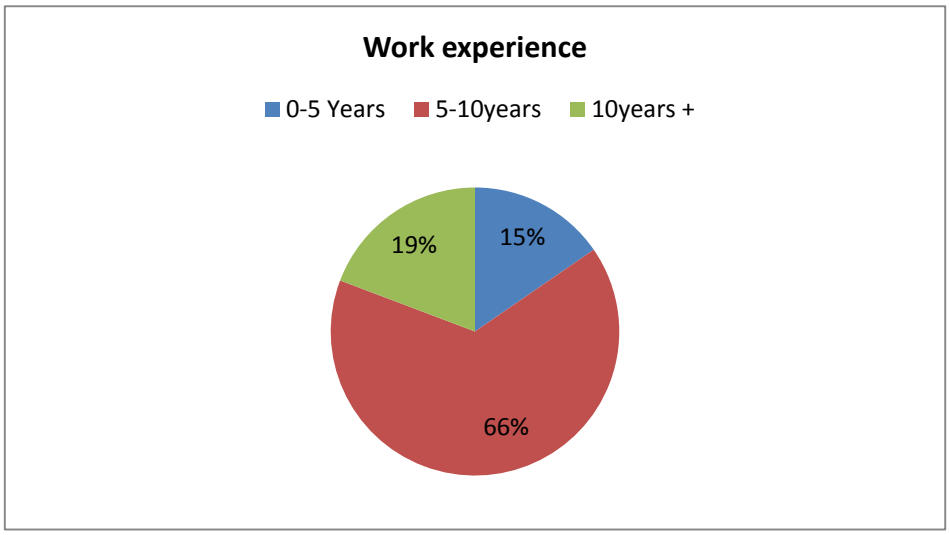
Figure 4.1.3: Distribution of educational qualifications of the respondents



Source: primary data, 2017

From the findings, it was indicated that majority of the respondents were Postgraduate degree holders 24 (46 %) while the least were certificate holders 2 (4%). The diploma holders were 8 (15%) and the Undergraduate degree holders were 18 (35%). The findings implied that Postgraduate degree holders had more knowledge about information security more than respondents with other qualifications.

Figure 4.1.4: showing distribution of working experience of the respondents



Source: primary data, 2017

As for the work experience, majority of the respondents had worked for between 5 - 10 years and these were 34 (66%) while those who had worked for 10 years plus were 10 (19%). Those who had worked between 0-5 years were 8 (15%). This implies that 44% had worked for more than 5 years.

4.2 Descriptive statistics

4.2.1 Descriptive statistics to analyze information security controls at KIU.

The researcher analyzed the information security controls at KIU.

Table 4.2.1.1: Shows the mean range which was used to arrive at the mean of the individual indicators and interpretation.

A five Likert scale was used in the questionnaires to obtain participant's preferences or degree of agreement with a statement or set of statements. Likert scales are non-comparative scaling technique and are unidimensional (only measure a single trait) in nature.

Mean Range	Response Mode	Interpretation
4.21-5.00	Strongly agree	Very High
3.41- 4.20	Agree	High
2.61-3.40	Neutral	Fair
1.81-2.60	Disagree	Low
1.00-1.80	Strongly disagree	Very Low

Table 4.2.1.2a): Descriptive statistics to establish information security controls in the Human Resource department of KIU.

No.	Categories	Mean	Std. Deviation	Cov.	Interpretation
1.	**Ongoing knowledge of attack sources, scenarios and techniques** KIU maintains an ongoing awareness of attack threats through security information sources	3.44	1.227	2.8.3	High
2.	All defensive measures are based on knowledge of the attacker's capabilities and goals.	3.33	1.167	2.853	Fair
3.	All defensive measures are based on probability of attack.	3.19	1.221	2.612	Fair
	Average	**3.3205**	**1.08859**	3.050	Fair
4.	**Up-to-date equipment inventories and network maps** KIU has inventories of machines and software sufficient to support timely security updates and audits.	3.52	1.180	2.983	High
5.	Inventories of hardware and software on each system can accelerate the institution's response to newly discovered vulnerabilities.	3.42	1.258	2.718	High
6.	The inventories support the proactive identification of unauthorized devices or software.	3.35	1.170	2.863	Fair
	Average	**3.4295**	**1.05891**	3.238	High
7.	**Rapid response capability to react to newly discovered vulnerabilities** Mitigation of the risks is by reconfiguring other computing devices.	3.35	1.046	3.202	Fair
8.	KIU has a reliable process to become aware of new vulnerabilities.	3.29	1.109	2.966	Fair
9.	The Institution usually responds rapidly to widely known security vulnerabilities	3.29	0.997	3.299	Fair
10.	KIU reacts as necessary to mitigate the risks posed by newly discovered vulnerabilities.	3.27	1.105	2.9599	Fair
11.	The institution’s Software is seldom flawless.	3.25	1.135	2.863	Fair
	Average	**3.2885**	**0.79746**	4.123	Fair
12.	**Network access controls over external connections** The Institution carefully controls external access through all channels including remote dial-up and VPN connections.	3.58	1.109	3.228	High
13.	Firewalls are used to enforce the institution's policy over traffic entering the institution's network.	3.35	1.203	2.784	Fair
	Average	**3.4615**	**1.05647**	3.276	High

Source: primary data, 2017

Table 4.2.1.2b): Descriptive statistics to establish information security controls at KIU

14.	**System hardening** The institution "hardens" its systems prior to placing them in a production environment.	3.48	1.111	3.132	High
15.	Computer equipment and software are frequently shipped from the manufacturer with default configurations and passwords.	3.29	1.160	2.836	Fair
	Average	**3.3846**	**0.93208**	3.631	Fair
16.	**Controls to prevent malicious code** The Institution maintains up-to-date virus definition files.	3.60	1.257	2.863	High
17.	KIU educates employees in safe computing practices, installing anti-virus software on servers and desktops etc.	3.38	1.388	2.435	Fair
18.	The Institution configures their systems to protect against the automatic execution of malicious code.	3.27	1.300	2.515	Fair
	Average	**3.4167**	**1.13159**	3.416	High
19.	**Rapid intrusion detection and response procedures** The Computing systems in place are perfectly secure.	3.46	1.075	3.218	High
20.	The institution has mechanisms in place to reduce the risk of undetected system intrusions.	3.37	1.121	3.006	Fair
	Average	**3.415**	**0.97378**	3.506	High
21.	**Physical security of computing devices** Access to those areas is restricted to administrative personnel	4.54	7.094	0.639	Very high
22.	The Institution's servers and network devices are placed in areas that are available only to specifically authorized personnel.	3.81	1.205	3.161	High
	Average	**4.1731 3**	**0.72970**	5.718	High
23.	**Authorized use policy** KIU has a written institutional policy that addresses the systems various accessibility, unsafe computing practices, and consequences for noncompliance.	3.29	1.258	2.615	Fair
24.	All internal system users and contractors are trained in and guided by the said policy.	3.19	1.103	2.892	Fair
	Average	**3.2404**	**1.07325**	3.019	Fair

Source: primary data, 2017

Table 4.2.1.2c): Descriptive statistics to establish information security controls at KIU.

25.	**Training** Periodically: KIU identifies and addresses training needs.	3.27	1.359	2.406	Fair
26.	KIU trains its personnel in the technologies they use.	3.21	1.333	2.408	Fair
27.	KIU trains its employees the institution's rules governing the use of specific technologies.	3.13	1.329	2.355	Fair
	Average	**3.2051**	**1.21385**	2.640	Fair
28.	**Independent testing**. The Institution ensures prompt corrective action where deficiencies are identified.	3.15	1.055	2.985	Fair
29.	The Institution provides independent assurance for compliance with security policies. Conduct periodic review of entry access journals and/or entry logbooks to verify that only authorized personnel are accessing space where computer systems are used.	3.12	1.215	2.567	Fair
30.	KIU possesses a testing plan that identifies control objectives.	3.10	1.225	2.530	Fair
31.	The institution schedules tests of the controls used to meet the said objectives.	3.06	1.178	2.597	Fair
32.	KIU ensures that hardcopy records and computer discs that are no longer useful are properly destroyed; preferably by shredding.	3.00	1.252	2.396	Fair
	Average **Total average mean**	**3.0846** **3.401**	**0.99516** **1.0046**	2.740	High

Source: primary data, 2017

The results in table 4.2.1.2a) - 4.2.1.2c) reveal that information security controls in KIU were rated as high with a total average mean of 3.401 in Kampala International University. The findings implied that majority of the respondents agreed with the statement that there are information security controls in KIU. There are information security controls to ensure the security of the University's records.

4.2.2 Descriptive statistics for exploring the extent of compliance to information security objectives at KIU.

The researcher explored the extent of compliance to information security objectives at KIU through the use of descriptive statistics.

Table 4.2.2.1a): Descriptive statistics to explore the extent of compliance to information security objectives in KIU.

No.	Categories	Mean	Std. Deviation	Cov	Interpretation
1.	**Confidentiality of records** The University has policies and procedures for handling information about clients, including confidentiality and data protection.	3.83	1.024	3.74	High compliance
2.	There measures at KIU that ensure that messages and data are available only to those who are authorized to view them.	3.67	1.248	2.94	High compliance
3.	KIU summons its staff to keep secret of both written and verbal communication from clients.	3.62	1.087	3.33	High compliance
4.	KIU protects the dignity and rights of its staff and minimizes the risk of harm that may happen to them.	3.33	1.133	2.939	Fair compliance
5.	At KIU, feelings of incompetence and the concomitant risk of embarrassment that can arise in everyday social situations are managed properly.	3.19	1.103	2.890	Fair compliance
	Average	**3.53**	**0.808**	**4.368**	High compliance
6.	**Integrity** KIU has got measures that ensure that information being displayed on a website, or transmitted or received over the internet, is not altered in any way by unauthorized parties.	3.73	0.972	3.837	High compliance
7.	The University has integrity policies that prevent accidental or malicious changes or the destruction of information.	3.46	0.828	4.178	High compliance
8.	Documents, information or data at KIU are used only by authorized people using authorized processes which include an audit trail that tracks its life cycle.	3.31	1.164	2.843	Fair compliance
9.	Data accuracy and completeness at the University is assured over its entire life-cycle.	3.25	1.027	3.164	Fair compliance
10.	Hashing the data you receive and comparing it with the hash of the original message is one of the methods used at KIU to protect data integrity.	3.23	1.096	2.947	Fair compliance
	Average	**3.04**	**0.718**	4.233	Fair compliance
11.	**Availability** At KIU information is made available when and where it is rightly needed	3.71	1.194	3.107	High compliance
12.	The property of being accessible and useable upon demand by an authorized entity is put into consideration.	3.48	1.111	3.132	High compliance
13.	KIU has policies that ensure proper functioning of all the components of information systems so that availability is maintained.	3.46	1.146	3.019	High compliance
14.	There is ensuring of timely and reliable access to and use of information at KIU.	3.44	1.018	3.379	High compliance
15.	KIU ensures data availability by use of backup to limit the damage caused by damage to hard drives or natural disasters.	3.35	1.235	2.712	Fair compliance
	Average	**3.49**	**0.918**	**3.801**	High compliance
16.	**Accountability** At KIU information is made available when and where it is rightly needed.	3.71	1.194	3.107	High compliance
17.	The property of being accessible and useable upon demand by an authorized entity is put into consideration.	3.48	1.111	3.132	High compliance
18.	KIU has policies that ensure proper functioning of all the components of information systems so that availability is maintained.	3.46	1.146	3.019	High compliance
19.	There is ensuring of timely and reliable access to and use of information at KIU	3.44	1.018	3.379	High compliance
20.	KIU ensures data availability by use of backup to limit the damage caused by damage to hard drives or natural disasters.	3.35	1.235	2.712	Fair compliance
	Average	**3.50**	**0.938**	3.731	High compliance

Source: primary data, 2017

Table 4.2.2.1b): Descriptive statistics to explore the extent of compliance to information security objectives in KIU.

21.	**Authentication** At KIU there are methods for proving that you are who you say you are.	3.67	1.184	3.099	High compliance
22.	There is verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system at KIU.	3.67	1.080	3.398	High compliance
23.	The University carries out authentication to confirm that the claimed characteristic of an entity is actually correct.	3.60	1.034	3.481	High compliance
24.	There is establishing confidence of authenticity at the University.	3.50	1.057	3.311	High compliance
25.	The University carries out, identity verification, message origin authentication, and message content authentication.	3.29	1.016	3.238	Fair compliance
	Average	**3.55**	**0.78727**	4.509	High compliance
26.	**Authorization** At KIU there is a process of ensuring that a user has sufficient rights to perform the requested operation and preventing those without sufficient rights from doing the same.	3.73	1.254	2.974	High compliance
27.	There is access privilege granted to a user, program, or process or the act of granting those privileges at the University.	3.67	1.080	3.398	High compliance
28.	There is use of commands after the user has logged into a system at the University.	3.50	1.180	2.966	High compliance
29.	There is determining what types or qualities of activities, resources, or services a user is permitted at KIU.	3.44	1.037	3.317	High compliance
30.	At the University, once you have authenticated a user, they may be authorized for different types of access or activity.	3.31	1.245	2.658	Fair compliance
	Average	**3.5231**	**0.82143**	4.288	High compliance
31.	**Non-repudiation** The University has properties of cryptographic digital signatures that offer the possibility of proving whether a particular message has been digitally signed by the holder of a particular digital signature's private.	3.29	1.035	3.178	Fair compliance
32.	There is capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message at KIU.	3.27	0.952	3.434	Fair compliance
33.	There is a security service by which the entities involved in a communication cannot deny having participated at the University.	3.12	1.149	2.715	Fair compliance
34.	KIU uses Non-repudiation to guarantee that people cannot deny that an event happened or an action was carried out by an entity.	3.12	0.922	3.383	Fair compliance
35.	There is a service that is used to provide assurance of the integrity and origin of data in such a way that the integrity and origin can be verified and validated by a third party as having originated from a specific entity in possession of the private key at KIU.	2.98	1.019	2.924	Fair compliance
	Average **Total average mean**	**3.1538** **3.40**	**0.79075** **0.826**	3.988 3.170	Fair compliance High compliance

Source: primary data, 2017

The results in table 4.2.2.1a) - 4.2.2.1b) reveal that there was high compliance to information security objectives in KIU with a total average mean of 3.40. The findings mean that majority of the respondents agreed with the statement of compliance to information security objectives in KIU.

4.2.3 Descriptive statistics to investigate challenges of information security of records in KIU.

The researcher investigated the challenges of information security of records in KIU.

Table 4.2.3.1: Descriptive statistics to investigate challenges of information security of records in KIU.

No.	Categories	Mean	Std. Deviation	Cov.	Interpretation
1.	Once vulnerability is discovered, cybercriminals can launch attacks on the institution.	3.33	1.216	2.738	Fair
2.	People unintentionally do something they shouldn't or not have the proper access controls on a system or the associated data.	3.27	1.223	2.673	Fair
3.	At KIU, malware has certainly evolved to become more sophisticated and dangerous than ever.	3.15	1.127	2.795	Fair
4.	There is resistance to embrace new products and technologies that emerge from "divergent thinking" at the institution.	3.02	1.276	2.366	Fair
5.	At KIU Cybercrime syndicates see value in exploiting network connectivity.	3.02	1.038	2.909	Fair
6.	Hackers steal login information then use the credentials to access applications and sensitive data.	2.96	1.371	2.159	Fair
7.	Cybercriminals find their way inside the institution's networks, they move laterally between applications until they find the most sensitive and valuable data.	2.87	1.284	2.235	Fair
8.	KIU uses mismatched, cobbled-together security solutions instead of one holistic product, which puts the institution's data at risk.	2.85	1.092	2.609	Fair
	Average mean	**3.0577**	**0.80800**	2.560	Fair

Source: primary data, 2017

The results in table 4.4.1 reveal that challenges of information security of records in KIU were rated as fair with a total average mean of 3.0577, Standard deviation 0.80800 in Kampala

International University. The findings mean that majority of the respondents' response was neutral. Respondents neither agreed nor disagreed with the statement that there challenges of information security of records in KIU, were not sure whether there were challenges to information security of records or not.

4.3 Establishment of the relationship between challenges of information security of records and information security objectives in KIU.

The level of significance between challenges of information security of records and security objectives in KIU was checked. The PLCC was used to determine if there was a significant relationship between challenges of information security of records and security objectives in KIU at 0.05 level of significance so as to enable the researcher to either accept or reject the null or alternate hypothesis.

Table 4.3.1: Significant relationship between challenges of information security of records in KIU and security objectives using Pearson Linear Correlation Co- efficiency (PLCC)

Variables	Mean	r–value	Sig value	Interpretation	Decision
Challenges of information security records Vs. information security objectives	3. 0577 3.40	0.105	0.460	insignificantly correlated	Null hypothesis accepted

Source: primary data, 2017

Table 4.3.1 shows the correlation between challenges of information security of records and security objectives in KIU at 0.105; this meant that the variables had a 10.5% relationship; there could be other factors affecting security objectives other than the challenges of information security. The average mean for challenges of information security of records in KIU was 3.0577 and 3.40 for security objectives. The significance was at 0.460 which was more than 0.05 the actual level of significance. The significance was 0.460 which implied that there was no relationship between challenges of information security of records and security objectives in KIU. The null hypothesis which stated that there was no significant relationship between challenges of information security of records and security objectives in Kampala International University was accepted and the alternate hypothesis rejected.

4.4 Regression analysis

The table below was the first table of interest while carrying out a Regression analysis for information security challenges and information security objectives.

Table 4.4.1: Model Summary for regression analysis of information security challenges and information security objectives

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.105[a]	0.011	-0.009	0.81154

a. Predictors: (Constant), OBJ

The R value represented that there was a low degree of correlation between the variables. The adjusted R2 represented the negative correlation at -0.009 between the intervening variable, information security challenges, and the dependent variable information security objectives. This implies that challenges negatively influence compliance or attainment of information security objectives. Nevertheless, the rate of change is very minimal at 0.001. Therefore, there could be a number of factors that were beyond the scope of this study that may account for the failure of 100% attainment of information security objectives within this study's context.

The other table was the Analysis of variance **(ANOVA)** table, which reported how well the regression equation fit the data.

Table 4.4.2: ANOVA for regression analysis of information security challenges and information security objectives

ANOVA

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	0.366	1	0.366	0.555	0.460[a]
	Residual	32.930	50	0.659		
	Total	33.296	51			

a. Predictors: (Constant), OBJ

b. Intervening Variable: CHAL

Table 4.4.2 indicates that the regression model which predicted that the intervening variable was not significant. In the "Regression" row at the "Sig." column it shows the significance at 0.460, which was more than 0.05, this meant that, overall regression model statistically did not significantly predict the outcome variable.

Table 4.4.3 Showing model summary for regression of information security controls and information security objectives

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.780[a]	0.609	0.601	0.39680

a. Predictors: (Constant), CONT

The adjusted R2 represented a positive correlation at 0.601 between the independent variable, information security controls and the dependent variable information security objectives. This also asserts that a perfect system of security controls will cause a 60.1% compliance or assurance of information security objectives.

Table 4.4.4: Analysis of variance (ANOVA) for regression of information security controls and information security objectives.

ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	12.248	1	12.248	77.790	0.000[a]
	Residual	7.872	50	0.157		
	Total	20.120	51			

a. Predictors: (Constant), CONT

b. Dependent Variable: OBJ

Table 4.6.4 indicates that the regression model predicted that the variables were significant. In the “Regression” row at the “Sig.” column it shows the significance at 0.000, which was less than 0.05, and indicate that, the overall regression model statistically did significantly predict the outcome variable.

CHAPTER FIVE

DISCUSSION OF FINDINGS, CONCLUSION AND RECOMMENDATIONS

5.0. Introduction

This chapter discusses the findings in chapter four in relation to the objectives of the study. It is subdivided into four sections. The first section presents and discusses information security controls, objectives and challenges to information security of records in KIU and also the relationship between compliance to information security objectives, and challenges to information security of records. The second section presents the conclusion. The third section presents the recommendations. The fourth section presents and suggests areas for further study.

5.1 Discussion of findings in relation to the objectives of the study

The findings obtained were explained in relation to the objectives of the study as indicated in the first chapter.

5.1.1 Objective one: To analyze the information security controls at Kampala International University, main campus, Kampala Uganda.

The findings indicated that majority of the respondents' response towards information security controls was rated as high (agreed) with Mean=3.401, S.d=1.0046. This meant that good record keeping with appropriate security measures is necessary. These findings were in line with a statement by Durbin (2016) that institutions need to have a reliable process so as to become aware of new vulnerabilities and to react as necessary to mitigate the risks posed by newly discovered vulnerabilities. Computer equipment and software are frequently shipped from the manufacturer with default configurations and passwords that are not sufficiently secure with in an institutional environment, this therefore requires hardening the systems prior to placing them in a production environment. He added that software is seldom flawless and that some of the flaws may represent security vulnerabilities and in some cases, management may mitigate the risk by reconfiguring other computing devices, there is need for rapid response because a widely known vulnerability is subject to an increasing number of attacks. System "hardening" is the process of removing or disabling unnecessary or insecure services and files, a number of organizations have current efforts under way to develop security benchmarks for various vendor systems (Fratto, 2007).

The findings are also in line with a report by Scarfone (2007) which states that when a security failure occurs and an attacker is "in" the institution's system, rapid detection and reaction can minimize any damage that might occur, techniques used to identify intrusions include intrusion

detection systems (IDS) for the network and individual servers (i.e., host computer), automated log correlation and analysis, and the identification and analysis of operational anomalies. Educating employees in safe computing practices, installing anti-virus software on servers and desktops, maintaining up-to-date virus definition files, and configuring systems protects against the automatic execution of malicious code, malicious code can deny or degrade the availability of computing services; steal, alter, or insert information; and destroy any potential evidence for criminal prosecution, types of malicious code include viruses, worms, and Trojan Horses (Ballou, 2003).

5.1.2 Objective two: To explore the extent of compliance to information security objectives at Kampala International University, main campus, Kampala, Uganda.

The findings indicated that majority of the respondents' response towards compliance to information security objectives was rated as high with a total average mean of 3.40 and S.d=0.826 in Kampala International University. The findings mean that majority of the respondents agreed with the statement that there is compliance to information security objectives in KIU. The findings were in line with a report by Alfawaz et al. (2008) which state that traditionally security is concerned with information properties of confidentiality, integrity and availability which strengthen user services such as accountability. The findings were also in line with Pahnila (2007) who argued that major threats to information security are caused by careless employees who do not comply with organizational information security policies and procedures.

5.1.3 Objective three: To investigate the challenges to information security of records at Kampala International University, main campus, Kampala Uganda.

The findings indicated that majority of the respondents' response towards challenges of information security of records was rated as fair (neutral) with Mean=3.0577, S.d=0.80800). This implied that there are some information security controls in place to ensure the security of the University's records. The findings agree with Gartner (2016) who noted that once cybercriminals find their way inside corporate networks, they're moving laterally between applications until they find the most sensitive and valuable data, cryptographic isolation and end-to-end encryption prevents lateral movement. One of the primary causes of most data breaches and security incidents are people unintentionally doing something they shouldn't or not having the proper access controls on a system or the associated data. These challenges can be addressed by properly classifying and encrypting data, having a security awareness training program and limiting access to systems and data as much as possible.

According to Durbin (2016), ever since the birth of the Internet, crime syndicates saw value in exploiting worldwide connectivity. Durbin (2016) explained further that they have big budgets, deep skill sets and sophisticated tools to circumvent many of the best cyber security solutions. Keeping an eye on these syndicates will be a key to information security success. Security Frankenstein is a major information security concern, in other words, by using mismatched, cobbled-together security solutions instead of one holistic product, organizations are putting data at risk. Businesses and associations should try to find a single cyber security solution that effectively meets all needs, such as one that combines cryptographic segmentation and role-based access control in a package that meets all information security needs.

5.1.4 Objective four: To ascertain if there was a significant relationship between challenges to information security of records and information security objectives in Kampala International University, main campus, Kampala, Uganda.

The findings indicated that there was no significant relationship between challenges to information security of records and security objectives in Kampala International University. The findings were in line with Tassabehji (2005) who noted that evaluating information security is based on the principles of confidentiality, accountability as well as integrity. This was also supported by Wangwe et al. (2009) who suggest that information security should be addressed to ensure information confidentiality and integrity. Although information security guidelines are of a prescriptive nature and imperative to the users, users often fail to apply them as intended. As a result, the guidelines are often not effective for the purpose of influencing human behaviour and attitudes. People are an important resource in coping with information security, as the success of an information security programme depends on the commitment from all users. If this commitment is not in place, the security mechanisms could be bypassed or diminished by employees. There are several beneficial effects of a security awareness programme: increased confidence, better protection, correctness and reliability of information, fewer internal undesired incidents, improved moral and detection capability and improved compliance with laws and regulations, an ambitious manner that to achieve effectiveness, information security should be transferred into tacit knowledge and unconscious consciousness.

5.2. Conclusion

According to the findings**,** there are a number of essential factors which information security experts have to identify as being essential if an organization wants to achieve information security. As far as security controls are concerned, KIU; should employ staff responsible for monitoring and evaluating the information systems, should have a disaster recovery plan; the

plan should document the procedures to recover and protect the university's records in the event of disaster.

For the case of compliance to Information Security objectives, KIU should ensure that information is not disclosed to unauthorized persons. As far as Information security challenges are concerned, KIU should consider implementing internal network security solutions such as encryption.

The researcher discovered that there was a relationship between information security and the functions of the Human Resource department since the researcher found out that the Human Resource department was responsible for ensuring confidentiality, integrity and availability of data and information stored in its system.

There was no significant relationship between information security objectives and challenges to information security of records at KIU, main campus. This is because the significance was 0.460 which was more than 0.05. The null hypothesis was accepted and the alternate hypothesis was rejected.

5.3 Recommendations

In line with the objectives; as for security controls, KIU;

i. Should set up a secure backup system to ensure records are safely stored and regularly backed up. Daily backups should be done particularly for vital records.

ii. Should have a disaster recovery plan. The plan should document the procedures to recover and protect the university's records in the event of disaster.

iii. Should implement integrity policies to prevent accidental or malicious changes or the destruction of information.

iv. Should employ staff responsible for monitoring and evaluating the information systems.

v. Should implement logging of session statistics and information usage for the purpose of authorization control, billing, trend analysis, resource utilization and capacity planning activities.

vi. Should have tight restrictions as far as access to the server room is concerned so as to avoid intruders from tampering with the system.

vii. Should maintain an ongoing awareness of attack threats through security information sources.

viii. Should have inventories of machines and software sufficient to support timely security updating and audits of authorized equipment and software.

ix. Should reduce the risks posed by malicious code by, among other things, educating employees in safe computing practices, installing anti-virus software on servers and desktops, maintaining up-to-date virus definition files, and configuring their systems to protect against the automatic execution of malicious code, should train its personnel in the technologies they use and the institution's rules governing the use of those technologies.

As for compliance to Information Security objectives, KIU;

i. Should ensure that information is not disclosed to unauthorized persons by ensuring that there is tight security in information based areas.

ii. Should protect information from being modified by unauthorized parties by ensuring password usage,

iii. Should make sure that information is made available when and where it is rightly needed,

iv. Should ensure that information is transparent so that it is possible to determine whether a particular use is appropriate under a given set of rules.

As for the Information security challenges, KIU;

i. Must "look beyond" malware if it hopes to improve on information security standards

ii. Should use Cryptographic isolation and end-to-end encryption to prevent lateral movement, should encourage its staff to embrace new products and technologies,

iii. Should consider implementing internal network security solutions such as encryption which might be the best defense in regard to information security.

5.4. Areas for further studies

The findings of the study indicated that there was no significant relationship between challenges of information security of records and information security objectives in KIU, main campus,

therefore future researchers should look at; information security and records management and archives management and information security.

REFERENCES

Ahuja, R (2001). "*Research methods"*, Prem Rawat, Jaipur, India

Albrechtsen, E. (2007). "*A qualitative study of users' view on information security*", Computers & Security, Vol. 26 No. 4, pp. 276-289.

Alfawaz, S., May, L and Mohanak, K. (2008). "*E-Government security in developing countries: A managerial conceptual framework*". Retrieved July 5, 2010, from www.irspm2008.bus.qut.edu.au/IRSPM-2008.pdf

Amin, M. E. (2005). "Social science research: *Conception, methodology and analysis"*, Makerere University, Kampala.

Anderson, R. (2001). "*Why information security is hard, "an economic perspective*", ACSAC '01: Proceedings of the 17th annual computer security applications conference, IEEE computer security, Washington, D.C

Andress, J. (2014). "The basics of information security: understanding the fundamentals of InfoSec in theory and practice". Syngress

Ballou, S. (2003). GSEC Practical Version 1.4b

Berghel, H. (2005). "*The two sides of ROI: Return on investment vs risk of incarceration*," communication of the ACM, vol.48 no.4, pp. 15-20

Bhaskar, S. M. and Ahson, S. I. (2008). "*Information Security: A practical Approach*." Oxford: Alpha Science International Ltd.

Bhatnagar, V. and Sharma, S. (2012). "Data Mining: A Necessity for Information Security," *Journal* of Knowledge Management Practice, vol. 13 no.1, pp.1-24.

Blakely, B., McDermott, E. and Geer, D. (2001). "*Information security is information risk management*", Proceedings of the 2001 Workshop on New Security Paradigms, ACM Press, New York, NY, pp. 97-104.

Boritz, J. Efrim (2011). "*IS Practitioners' Views on Core Concepts of Information Integrity*". International Journal of Accounting Information Systems. Elsevier. Retrieved 12 August.

Brown, J. (2007). Calculating Reliability

Brown, J. S. and Duguid, P. (2002). "*The Social Life of Information*." Boston, Harvard Business School Press.

Burd, S. A. (2005). *"Information security in academic institutions",* Metro InfraGard Membership Alliance, Inc., New York

Cherdantseva, Y. and Hilton, J. (2013). "*Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals"*. In: Organizational, Legal, and Technological Dimensions of Information System Administrator. Almeida, F., Portela, I. (eds.). IGI Global Publishing.

Clark, C. (2006). Journal of Social Work 6(2): 117–136, Sage Publications, London

Conklin, W. A. (2007). Barriers to Adoption of e-Government. *Proceedings of the 40th* Hawaii International Conference on System Sciences – 2007. Pp. 1–8.

Creswell, J. W. (2009). *"Research design: Qualitative, quantitative and mixed methods approaches"*, Sage, London

Demopoulos, T. (2002). *Making information and the internet work*, Demopoulos Associates, USA, www.demop.com

Doherty, N. F. and Fulford, H. (2006). "*Aligning the information security policy with the strategic information systems plan*", Computers & Security, vol. 25 no. 1, pp. 55-63.

Doherty, N. F. and Fulford, H. (2005). *Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis*. Information Resources Management Journal, vol. 18, no. 2, pp. 21-39.

Dorey, P. (2007). D*igital business security*, Bp PLC, UK

Federal Financial Institutions Examination Council (FFIEC) (2006). "*Information Security (IS)* Federal Financial Institutions Examination Council (FFIEC)" *July* (*2006*). *IT Examination Handbook*. US

Fratto, M (2007). "Network Computing"

Smith, G. (2000). "*Love Bug' victims don't want a cure",* The Wall Street Journal (May 8), A42.

Garbars, K (2002). "*Implementing an Effective IT security Program".* SANS Institute, As part of the information security reading room. GSEC Version 1.4.

Gibson, S. and Benson, O. (2012). "Article, talking about suicide: *Confidentiality and anonymity* in qualitative research", sage, UK

Glaessner, T., Kellermann, T., and McNevin, V.(2002). "Electronic Security: Risk Mitigation in Financial Transactions Public Policy Issues, Department of the Treasury", USA

Gordon, L. A. and Loeb M.P. (2001). "A framework for using information security as a response to competitor analysis systems", Communications of the ACM 44(9), 70–75.

Gordon, LA & Loeb, MP (2002). "*The economics of information security investment*", ACM Transactions on Information and System Security (TISSEC), Vol. 5 No. 4, pp. 438-57.

Gordon, LA & Loeb, MP (2006). "*Budgeting Process for Information Security Expenditures."* Communications of the ACM, Vol. 49, No. 1, pp. 121-125.

Hind, S (2002). "*Security Surveys Spring Crop."* Computers and Security, Vol. 21, No. 4, pp. 310-321.

Ho¨ne, K & Eloff, JHP (2002). "*Information security policy – what do international security standards say?*" Computers & Security, Vol. 21 No. 5, pp. 402-9.

Jacobs, S (2011). Engineering information security: the application of systems engineering concepts to achieve information assurance, institute of electrical and electronics engineers

JNSA (2010). *survey report for the information security incident in 2009*, Japan Network security Association, Tokyo, www.jnsa.org/result/incident/2009.html Journal of Information Development is published quarterly, 2001, NSW Sydney Australia

Johnson, E (2006). "*Awareness training, security awareness: switch to a better programme*", Network Security, Vol. 2006 No. 2, pp. 15-18.

Jøsang, A (2017). A Consistent Definition of Authorization, Proceedings of the 13th International Workshop on Security and Trust Management (STM 2017)

Kabay, ME (2004). *What's Important for Information Security*: a Manager's Guide, Wiley, New York

Kagal, L, Hanson, C, & Weitzner, D (2008). Integrated policy explanations via dependency tracking. In *Proceedings of the IEEE Workshop on Policies for Distributed Systems and Networks* (June 2–4, 2008).

Karyda, M, Kiountouzis, E & Kokolakis, S (2005). "*Information systems security policies: a contextual perspective*", Computers & Security, Vol. 24 No. 3, pp. 246- 60.

Kaufman, BE (2008). *Managing the Human Factor: The Early Years of Human Resource Management in American Industry. Ithaca, New York: Cornell University Press*

Kedrosky, P (2000). "*Hackers prey on our insecurities",* The Wall Street Journal (February 10), A18

Kemp, M (2005). "*Beyond trust: security policies and defence in depth*", Network Security, Vol. 2005 No. 8, pp. 14-16.

Keyser, T & Dainty C (2004). *Information management and computer security*, British Computer Society, Britain

Komatsu, A, Takagi, D, & Matsumoto, T (2010). Empirical study on cognitive structures and personal gain in information security counter measure, journal of IPSJ, Vol. 51 pp. 1711- 25

Kurtz, G, (2016). Journal of Healthcare Information Management, Vol. 17, No. 3, www.providersedge.com/ehdocs/ehr_articles/EMR_Confidentiality_and_Information_Security.pdf

Kurtz, G (2016). Computer Business Review

Labuschagne, L & Eloff, JHP (2000). *Information Management & Computer Security*, Volume 8 , issue 3, Electronic commerce: the information-security challenge, pp: 154-157, MCB UP Ltd, ISSN: 0968-5227

Lampson, BW (2002). "Computer Security in the Real World. Principles of Computer Systems." www.research.microsoft.com/lampson.

Laudon, KC & Traver, CG (2008). *E-Commerce: business*, *technology*, society, 4th ed., Pearson Education, Inc., U.S.A

Layton, TP (2007). Information Security: Design, Implementation, Measurement, and Compliance. Boca Raton, FL: Auerbach publications.

Lobree, B (2002), "*Impact of legislation on information security management*", Security Management Practices, November/December, pp. 41-8.

Lutaaya, S (2015). "Corporate Records and Archives References Services: challenges and opportunities from the Bank of Uganda perspective". Kampala: Board Affairs Department

Madigan, EM, Petrulich, C and Motuk, K (2004). "*The cost of Non-Compliance-When Policies Fail*." Proceedings of the 32nd annual ACM SIGUCCS conference on User services, pp. 47 – 51, USA.

Mnjama, N (2005). "Archival landscape in Eastern and Southern Africa, LibraryManagement, 26(8/9):457-470"

Moore, R (2005). *"Cybercrime: Investigating High-Technology Computer Crime*," Cleveland, Mississippi: Anderson Publishing.

Mubazi, J (2009). Research methods, Faculty of Economics and Management Makerere University, Kampala

Mugenda, OM & Mugenda, AG (1999). Research methods: quantitative and qualitative approaches, Acts Press, Nairobi

Nevias, K (2016). Information technology & risk management, NJ

Obaidat, M & Boudriga, N (2009), *Security of e-systems and computer networks,* Cambridge university press.

Odongtho, C (2006). Mulago Hospital had no Computerized Patient Record System, article, Uganda Radio Network

Oso, WY & Onen, D (2009). A general guide to writing research proposal and report: a handbook of beginning researchers, rev. ed., The Jomo Kenyatta foundation, Nairobi

Pahnila, S, Siponen, M & Mahmood, A (2007).Which factors explain employee's adherence to information security policies?An empirical study,PACIS proceedings 73

Peltier, TR (2002). Information Security Policies, Procedures, and Standards: guidelines for effective information security management. Boca Raton, FL: Auerbach publications

Pfleeger, CP (1997). "*Security in Computing."* Prentice Hall PTR.2nd Edition.

Power, R, CSI/FBI, (2002). "*Computer Crime and Security Survey*", Computer Security Issues and Trends 18(2), 7–30.

Rahman, NNB & Widyarto, S (2013). Information Security: Human Resources Management and Information Security Incident Management, Palembang, Indonesia

Rouse, M (2007). *Security network security*, McGraw-Hill, New York

Rouse, M (2010). *Security network security*, McGraw-Hill, New York

Sandhu, R (2003). "Good-Enough Security Toward a Pragmatic Business-Driven Discipline." IEEE Computing Society.

Scarfone, K & Mell, P (2007). Guide to Intrusion Detection and Prevention Systems (IDPS); Report Number: 800-94; NIST Special Publication: Gaithersburg, MD, USA

Schiller, JI (2002). Security on Campus: An Interview; Technology for Higher Education Volume 16, No. 1. (2002): pg 12-14.

Schlienger, T & Teufel, S (2002). Information security culture the socio-cultural dimension in Information security management. FIPTCII international conference on information security; 7-9 May 2002

Schein, EH (2004). *Organizational culture and leadership*. Hoboken, John Wiley & Sons, Inc.

Schneier, B (2000). "Secrets and Lies. Digital Security in a Networked World", Wiley, Indianapolis, IN.

Schou, C & Shoemaker, D (2007). Information assurance for the enterprise: a roadmap to information security, McGraw-Hill/Irwin, New York

Schuessler, JH (2009). General deterrence theory: assessing information systems security effectiveness in large versus small businesses journal within an information security context," Master's thesis, Department of the Air Force

Scott, S (2018). Six Main Functions of a Human Resource Department

Shabtai, A, Elovici, Y & Rokach, L (2012). Introduction to Information Security. In *A Survey of Data Leakage Detection and Prevention Solutions* (pp. 1-4). Springer US.

Shardlow, (1995). *Against confidentiality? Privacy, safety and the public good in professional communications*, Sage, London, 2006, www.sagepublications.com Journal of social work 6(2):117-136

Siponen, MT & Oinas-Kukkonen, H (2007). "*A review of information security issues and respective research contributions*", The Database for Advances in Information Systems, Vol. 38 No. 1, pp. 60-81.

Solove, D (2004). *The Digital Person.* New York University Press, New York,

Spafford, E (2007). *Computer security: a computer is secure if you can depend on it and its software to behave as you expect*, Purdue University center for education and research in information assurance and security (CERIAS), USA

Straub, D, Loch, K & Hill (2001). Transfer of information technology to the Arab world: a test of cultural influence modeling journal of global information management, 9:6-28

Straub, DW & Welke, RJ (1998). "Coping with System Risk: Security Planning Models for Management decision Making." MIS Quarterly, Vol. 22, No. 4, pp. 441-470.

Sundt, C (2006). *"Information security and the law*", Information security technical report, Vol. 11 No. 1, pp. 2-9.

Szomszor, M & Moreau, L (2003). Recording and reasoning over data provenance in Web and grid services. In *Proceedings of the International Conference on Ontologies, Databases, and Applications of Semantics 2888* (Catania, Sicily, Italy, 2003), 603–620.

Taherdoost, H, Chaeikar, SS, Jafari, M, & Shojae Chaei Kar, N (2013). Definitions and Criteria of CIA Security Triangle in Electronic Voting System. *International Journal of Advanced Computer Science and Information Technology (IJACSIT) Vol*, *1*, 14-24.

Tassabehji, R (2005). Inclusion in E-Government: A Security Perspective. *E- Government Workshop'05(eGov05)*, Brunel University, UK. pp. 1-9.

Theoharidou, M, S Kokolakis, et al. (2005). "The insider threat to information systems and the effectiveness of ISO17799." Computers & Security 24: 472-484.

Thomson, KL & Von Solms, R (2006). "*Towards an information security competence maturity model*", Computer Fraud & Security, Vol. 2006 No. 5, pp. 11-15.

Tipton, HF & Krause, M (2007). Information security handbook, 6th ed., CRC Press

Vigo, R (2011). *"Representational information: a new general notion and measure of information"*. Information Sciences, 181 (2011), 4847-4859, Routledge, New York

Von Solms, R 1996. "Information Security Management: The Second Generation". Computer & Security, Vol. 15, pp. 281-288.

Von Solms, B (2000). "*Information security – the third wave?*" Computer & Security, Vol. 19 No. 7, pp. 615-20.

Von Solms, B (2006). "*Information security – the fourth wave*", Computer & Security, Vol. 25 No. 3, pp. 165-8.

Wangwe, CK, Eloff, MM, & Venter, LM (2009). E-Government Readiness: An Information Security Perspective from East Africa. *Proceedings of IST-Africa 2009* Conference. pp. 1–6.

Ward, P & Smith, CL (2002). "*The development of access control policies for information technology systems*", Computer & security, Vol. 21 No. 4, pp. 365-71.

Wiant, TL (2005). "*Information security policy's impact on reporting security incidents*", Computer &security, Vol. 24 No. 6, pp. 448-59.

Whitman, ME (2003). "*Enemy at the Gate: Threats to Information Security*." Communications of the ACM, Vol. 46, No. 8, pp. 91-95.

Whitman, ME., Caylor, J, Fendler, P & Baker, D (2005). *Rebuilding the Human Firewall.* Information Security Curriculum Development Conference, Kennesaw, GA, USA. ACM, pp. 104-106

Wright, J & Jim, H (2009). *Computer and Information Security Handbook,* Morgan Kaufmann Publications Elsevier Inc p. 257.

Zhou, Z & Hu, C (2008). Study on the E-government Security Risk Management. *International*

APPENDICES

APPENDIX I: CONSENT FORM

I am giving my consent to be part of the research study of Ms. Mbabazi Stella that will focus on examining information security controls in the Human Resource Department of Kampala International University, Uganda.

I shall be assured of privacy, anonymity and confidentiality and that I will be given the option to refuse participation and right to withdraw my participation at any time I feel like doing so.

I have been informed that the research is voluntary and the results will be given to me in case I requested for them.

Initials: ——————————

Date ——————————————

APPENDIX II: QUESTIONNAIRE

Dear respondents,

I am glad to have you selected as a respondent to my study, examining information security controls in the Human Resource Department of Kampala International University, Uganda. Your observations, experience and opinions will be very important. This research is purely for academic purpose and intended to obtain information about the topic mentioned above. The data obtained will be treated with total confidentiality. Kindly complete this questionnaire and submit it to me.

Part I

Profile of respondents

Please tick in the boxes provided as your response ☐

1. Gender:
    - Male ☐
    - Female ☐
2. Age:
    - 20 – 29 ☐
    - 30 – 49 ☐
    - 50 and above ☐
3. Educational Qualifications :
    - Certificate ☐
    - Diploma ☐
    - Undergraduate degree ☐
    - Post graduate degree ☐
4. Work experience (in years)

Part II: An assessment of security controls, information security challenges and compliance to information security objectives in Kampala International University.

Please write your answers to the statements below. Kindly use the rating as guided below.

Response mode	Interpretation
5. Strongly agree	you agree with no doubt
4. Agree	you agree with some doubt
3. Neutral	you neither agree nor disagree
2. Disagree	you disagree with some doubt
1. Strongly disagree	you disagree with no doubt

Please tick the blanks provided as you respond

No.	Scale	5	4	3	2	1
	Information security objectives **Confidentiality of records**					
1.	There measures at KIU that ensure that messages and data are available only to those who are authorized to view them.					
2.	At KIU, feelings of incompetence and the concomitant risk of embarrassment that can arise in everyday social situations are managed properly.					
3.	KIU protects the dignity and rights of its staff and minimizes the risk of harm that may happen to them.					
4.	KIU summons its staff to keep secret of both written and verbal communication from clients.					
5.	The University has policies and procedures for handling information about clients, including confidentiality and data protection.					
	Integrity					
6.	KIU has got measures that ensure that information being displayed on a website, or transmitted or received over the internet, is not altered in any way by unauthorized parties.					
7.	The University has integrity policies that prevent accidental or malicious changes or the destruction of information.					
8.	Data accuracy and completeness at the University is assured over its entire life-cycle.					
9.	Documents, information or data at KIU are used only by authorized people using authorized processes which include an audit trail that tracks its life cycle.					
10.	Hashing the data you receive and comparing it with the hash of the original message is one of the methods used at KIU to protect data integrity.					
	Availability					
11.	At KIU information is made available when and where it is rightly needed.					
12.	KIU has policies that ensure proper functioning of all the components of information systems so that availability is maintained.					
13.	KIU ensures data availability by use of backup to limit the damage caused by damage to hard drives or natural disasters.					
14.	There is ensuring of timely and reliable access to and use of information at KIU.					
15.	The property of being accessible and useable upon demand by an authorized entity is put into consideration.					
	Accountability					
16.	The University has processes that measure the resources a user consumes during access.					
17.	Logging of session statistics and usage information is carried out at the university and used for authorization control, billing, trend analysis, resource utilization and capacity planning activities.					
18.	The University ensures that the use of information is transparent so that it is possible to determine whether a particular use is appropriate under a given set of rules.					
19.	At KIU, accountability involves being answerable for the actions and decisions that have been assigned.					
20.	The university entrusts an individual with the responsibility to safeguard and control, keying material, and information and also that individual being answerable to authority for the loss or misuse of that equipment or information.					
	Authentication					
21.	At KIU there are methods for proving that you are who you say you are.					
22.	The University carries out authentication to confirm that the claimed characteristic of an entity is actually correct.					
23.	There is verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system at KIU.					
24.	There is establishing confidence of authenticity at the University.					
25.	The University carries out, identity verification, message origin authentication, and message content authentication.					
	Authorization					
26.	At KIU there is a process of ensuring that a user has sufficient rights to perform the requested operation and preventing those without sufficient rights from doing the same.					
27.	There is access privilege granted to a user, program, or process or the act of granting those privileges at the University.					
28.	There is determining what types or qualities of activities, resources, or services a user is permitted at KIU.					
29.	There is use of commands after the user has logged into a system at the University.					
30.	At the University, once you have authenticated a user, they may be authorized for different types of access or activity.					
	Non-repudiation					
31.	The University has properties of cryptographic digital signatures that offer the possibility of proving whether a particular message has been digitally signed by the holder of a particular digital signature's private.					
32.	KIU uses Non-repudiation to guarantee that people cannot deny that an event happened or an action was carried out by an entity.					
33.	There is capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message at KIU.					
34.	There is a service that is used to provide assurance of the integrity and origin of data in such a way that the integrity and origin can be verified and validated by a third party as having originated from a specific entity in possession of the private key at KIU.					
35.	There is a security service by which the entities involved in a communication cannot deny having participated at the University					

Please tick the blanks provided as you respond

No.	Scale	5	4	3	2	1
	Information security controls					
	Ongoing knowledge of attack sources, scenarios and techniques					
1.	KIU maintains an ongoing awareness of attack threats through security information sources.					
2.	All defensive measures are based on knowledge of the attacker's capabilities and goals.					
3.	All defensive measures are based on probability of attack.					
	Up-to-date equipment inventories and network maps					
4.	KIU has inventories of machines and software sufficient to support timely security updates and audits.					
5.	Inventories of hardware and software on each system can accelerate the institution's response to newly discovered vulnerabilities.					
6.	The inventories support the proactive identification of unauthorized devices or software					
	Rapid response capability to react to newly discovered vulnerabilities					
7.	KIU has a reliable process to become aware of new vulnerabilities.					
8.	KIU reacts as necessary to mitigate the risks posed by newly discovered vulnerabilities.					
9.	The institution's Software is seldom flawless.					
10.	Mitigation of the risks is by reconfiguring other computing devices.					
11.	The Institution usually responds rapidly to widely known security vulnerabilities					
	Network access controls over external connections					
12.	The Institution carefully controls external access through all channels including remote dial-up and VPN connections.					
13.	Firewalls are used to enforce the institution's policy over traffic entering the institution's network.					
	System hardening					
14.	The institution "hardens" its systems prior to placing them in a production environment.					
15.	Computer equipment and software are frequently shipped from the manufacturer with default configurations and passwords.					
	Controls to prevent malicious code					
16.	KIU educates employees in safe computing practices, installing anti-virus software on servers and desktops etc.					
17.	The Institution maintains up-to-date virus definition files.					
18.	The Institution configures their systems to protect against the automatic execution of malicious code.					
	Rapid intrusion detection and response procedures					
19.	The institution has mechanisms in place to reduce the risk of undetected system intrusions.					
20.	The Computing systems in place are perfectly secure.					
	Physical security of computing devices					
21.	The Institution's servers and network devices are placed in areas that are available only to specifically authorized personnel.					
22.	Access to those areas is restricted to administrative personnel.					
	Authorized use policy					
23.	KIU has a written institutional policy that addresses the systems various accessibility, unsafe computing practices, and consequences for noncompliance.					
24.	All internal system users and contractors are trained in and guided by the said policy.					
	Training					
25.	**Periodically:** KIU identifies and addresses training needs.					
26.	KIU trains its personnel in the technologies they use.					
27.	KIU trains its employees the institution's rules governing the use of specific technologies.					
	Independent testing.					
28.	KIU possesses a testing plan that identifies control objectives.					
29.	The institution schedules tests of the controls used to meet the said objectives.					
30.	The Institution ensures prompt corrective action where deficiencies are identified.					
31.	The Institution provides independent assurance for compliance with security policies. Conduct periodic review of entry access journals and/or entry logbooks to verify that only authorized personnel are accessing space where computer systems are used.					
32.	KIU ensures that hardcopy records and computer discs that are no longer useful are properly destroyed; preferably by shredding.					

Please tick the blanks provided as you respond

No.	Scale	5	4	3	2	1
	Information security challenges					
	Compromised credentials and device:					
1.	At KIU, malware has certainly evolved to become more sophisticated and dangerous than ever.					
2.	Hackers steal login information then use the credentials to access applications and sensitive data.					
	Lateral hacker movement/breach containment:					
3.	Cybercriminals find their way inside the institution's networks, they move laterally between applications until they find the most sensitive and valuable data.					
	Stitched-together security:					
4.	KIU uses mismatched, cobbled-together security solutions instead of one holistic product, which puts the institution's data at risk.					
	Vulnerabilities can turn into intrusion points:					
5.	Once vulnerability is discovered, cybercriminals can launch attacks on the institution.					
	The age of cybercrime syndicates:					
6.	At KIU Cybercrime syndicates see value in exploiting network connectivity.					
	Resistance to embrace new products and technologies:					
7.	There is resistance to embrace new products and technologies that emerge from "divergent thinking" at the institution.					
	Other challenges in Information Security are people and access control.					
8.	People unintentionally do something they shouldn't or not have the proper access controls on a system or the associated data.					